

EXH. 1

(12) **United States Patent**
Ghosh et al.(10) **Patent No.:** US 8,839,422 B2
(45) **Date of Patent:** Sep. 16, 2014(54) **VIRTUAL BROWSING ENVIRONMENT**(75) Inventors: **Anup K Ghosh**, Centreville, VA (US); **Sushil Jajodia**, Oakton, VA (US); **Yih Huang**, Fairfax, VA (US); **Jiang Wang**, Fairfax, VA (US)(73) Assignee: **George Mason Research Foundation, Inc.**, Fairfax, VA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 565 days.

(21) Appl. No.: 12/827,203

(22) Filed: Jun. 30, 2010

(65) **Prior Publication Data**

US 2011/0167492 A1 Jul. 7, 2011

Related U.S. Application Data

(60) Provisional application No. 61/221,749, filed on Jun. 30, 2009.

(51) **Int. Cl.**

G06F 21/00 (2013.01)
H04L 29/06 (2006.01)
G06F 9/54 (2006.01)
G06F 21/56 (2013.01)
G06F 21/53 (2013.01)

(52) **U.S. Cl.**

CPC **G06F 9/54** (2013.01); **G06F 21/56** (2013.01);
H04L 63/1483 (2013.01); **G06F 21/53** (2013.01)

USPC 726/22; 713/188

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,211,871 B1 * 4/2001 Himmel et al. 715/744
 6,832,120 B1 12/2004 Frank et al.

7,552,479	B1 *	6/2009	Conover et al.	726/24
7,584,503	B1 *	9/2009	Palmer et al.	726/9
7,693,991	B2	4/2010	Greenlee et al.	
7,840,801	B2	11/2010	Berger et al.	
7,899,867	B1	3/2011	Sherstinsky et al.	
7,979,889	B2	7/2011	Gladstone et al.	
8,001,606	B1	8/2011	Spertus	
8,078,740	B2	12/2011	Franco et al.	
8,290,763	B1	10/2012	Zhang	
8,468,600	B1	6/2013	Kaskel et al.	
8,479,286	B2	7/2013	Dalcher et al.	
8,572,735	B2	10/2013	Ghosh et al.	

(Continued)

OTHER PUBLICATIONS

Huang, Yih; Stavrou, Angelos; Ghosh, Anup; Jajodia, Sushil; Efficiently Tracking Application Interactions using Lightweight Virtualization to Huang et al. Oct. 31, 2008; ACM; 9 pages.*

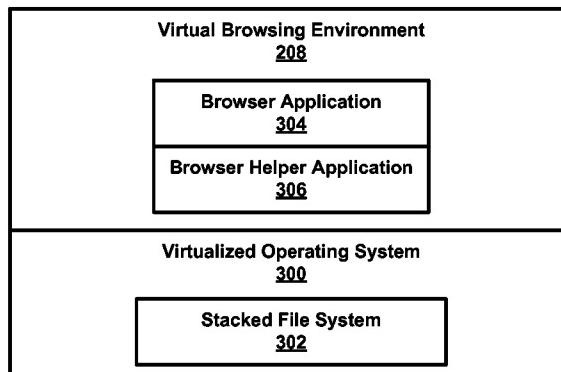
(Continued)

Primary Examiner — Gilberto Barron, Jr.*Assistant Examiner* — Malcolm Cribbs

(57)

ABSTRACT

An embodiment for providing a secure virtual browsing environment includes creating a virtual browsing environment with a virtualized operating system sharing an operating system kernel of a supporting operating system and executing the browser application within the virtual browsing environment. Another embodiment includes receiving a website selection within a browser application, determining if the website selection corresponds to a secure bookmark, and creating a second virtual browsing environment and executing the browser application within the second virtual browsing environment to access the website selection when the website selection corresponds to a website specified as a secure bookmark. Yet another embodiment includes monitoring operation of the operating system within the at least one virtual browsing environment, determining when the operation of the operating system includes potential malicious activity, and terminating the virtual browsing environment when the operation includes potential malicious activity.

20 Claims, 12 Drawing Sheets

US 8,839,422 B2

Page 2

(56)

References Cited**U.S. PATENT DOCUMENTS**

- 2004/0008652 A1 1/2004 Tanzella et al.
 2004/0025158 A1 2/2004 Traut
 2004/0064735 A1 4/2004 Frazier et al.
 2004/0093372 A1 5/2004 Chen et al.
 2005/0160133 A1 7/2005 Greenlee et al.
 2006/0021029 A1 1/2006 Brickell et al.
 2006/0136720 A1 6/2006 Armstrong et al.
 2006/0168156 A1 7/2006 Bae et al.
 2006/0271661 A1 11/2006 Qi et al.
 2006/0294519 A1 12/2006 Hattori et al.
 2007/0044151 A1 2/2007 Whitmore
 2007/0079307 A1 4/2007 Dhawan et al.
 2007/0107058 A1 5/2007 Schuba et al.
 2007/0192866 A1* 8/2007 Sagoo et al. 726/24
 2007/0240212 A1 10/2007 Matalytski
 2007/0271610 A1 11/2007 Grobman
 2007/0289019 A1 12/2007 Lowrey
 2008/0016339 A1 1/2008 Shukla
 2008/0059556 A1 3/2008 Greenspan et al.
 2008/0082976 A1 4/2008 Steinwagner et al.
 2008/0141266 A1 6/2008 Hunt et al.
 2008/0244747 A1* 10/2008 Gleichauf et al. 726/25
 2008/0320594 A1 12/2008 Jiang
 2009/0044265 A1 2/2009 Ghosh et al.
 2009/0125902 A1 5/2009 Ghosh et al.
 2009/0158432 A1* 6/2009 Zheng et al. 726/24
 2009/0300739 A1 12/2009 Nice et al.
 2009/0328008 A1 12/2009 Mital et al.
 2010/0064039 A9 3/2010 Ginter et al.
 2010/0115621 A1* 5/2010 Staniford et al. 726/25
 2010/0122342 A1 5/2010 El-Moussa et al.
 2010/0122343 A1 5/2010 Ghosh et al.
 2010/0125903 A1 5/2010 Devarajan et al.
 2010/0138639 A1 6/2010 Shah et al.
 2010/0223613 A1 9/2010 Schneider
 2011/0047620 A1 2/2011 Mahaffey et al.
 2011/0099620 A1 4/2011 Stavrou et al.
 2012/0297457 A1 11/2012 Schulte et al.
 2013/0145463 A1 6/2013 Ghosh et al.

OTHER PUBLICATIONS

Royal et al., PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. Computer Security Applications

Conference, 2006. ACSAC '06. 22nd Annual [online], Dec. 2006 [retrieved Apr. 4, 2014], Retrieved from the internet:< URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4041175> >.* Sapuntzakis, et al., "Virtual Appliances for Deploying and Maintaining Software," [online] (2003), ACM, pp. 1-15, Retrieved from the Internet. Adabala et al, From virtualized resources to virtual computing grids: the In-VIGO system. [online] (Nov. 11, 2003), Elsevier, pp. 1-14. Retrieved from the Internet: <<http://users.cis.fiu.edu/~zhaom/research/fgcs.pdf>>. Huang, Y. et al., "Efficiently tracking application interactions using lightweight virtualization," ACM, Oct. 31, 2008, 9 pages. International Search Report and Written Opinion mailed Mar. 12, 2013 for International Application No. PCT/US2012/067311. Office Action for U.S. Appl. No. 12/037,412, mailed Aug. 16, 2013. Final Office Action for U.S. Appl. No. 12/037,412, mailed Apr. 23, 2012. Office Action for U.S. Appl. No. 12/037,412, mailed Oct. 27, 2011. Office Action for U.S. Appl. No. 12/059,454, mailed Feb. 2, 2011. Final Office Action for U.S. Appl. No. 12/059,454, mailed Oct. 12, 2011. Office Action for U.S. Appl. No. 12/558,841, mailed Apr. 3, 2012. Office Action for U.S. Appl. No. 12/558,841, mailed Jan. 30, 2013. Office Action for U.S. Appl. No. 12/757,675, mailed Aug. 2, 2012. Office Action for U.S. Appl. No. 12/757,675, mailed May 15, 2013. Office Action for U.S. Appl. No. 13/296,319, mailed Dec. 17, 2012. Office Action for U.S. Appl. No. 13/296,319, mailed Sep. 5, 2013. Office Action for U.S. Appl. No. 13/690,452, mailed Nov. 8, 2013. Peterson et al., "A Flexible Containment Mechanism for Executing Untrusted Code," [online] (2002). University of California, pp. 207-225. Retrieved from the Internet: <<http://mse.uk.distfiles.macports.org/sites/ftp.wiretapped.net/pub/security/development/secure-programming/peterson-et-al-2002-a-flexible-containment-mechanism-for-executing-untrusted>>. Ugurlu, "Stealth Sandbox Analysis of Malware," PhD Thesis, Bilkent University (Ankara, Turkey) [online], Published Aug. 2009 [retrieved on Feb. 7, 2013] Retrieved from the Internet <URL: <http://www.thesis.bilkent.edu.tr/0003921.pdf>>.

* cited by examiner

U.S. Patent

Sep. 16, 2014

Sheet 1 of 12

US 8,839,422 B2

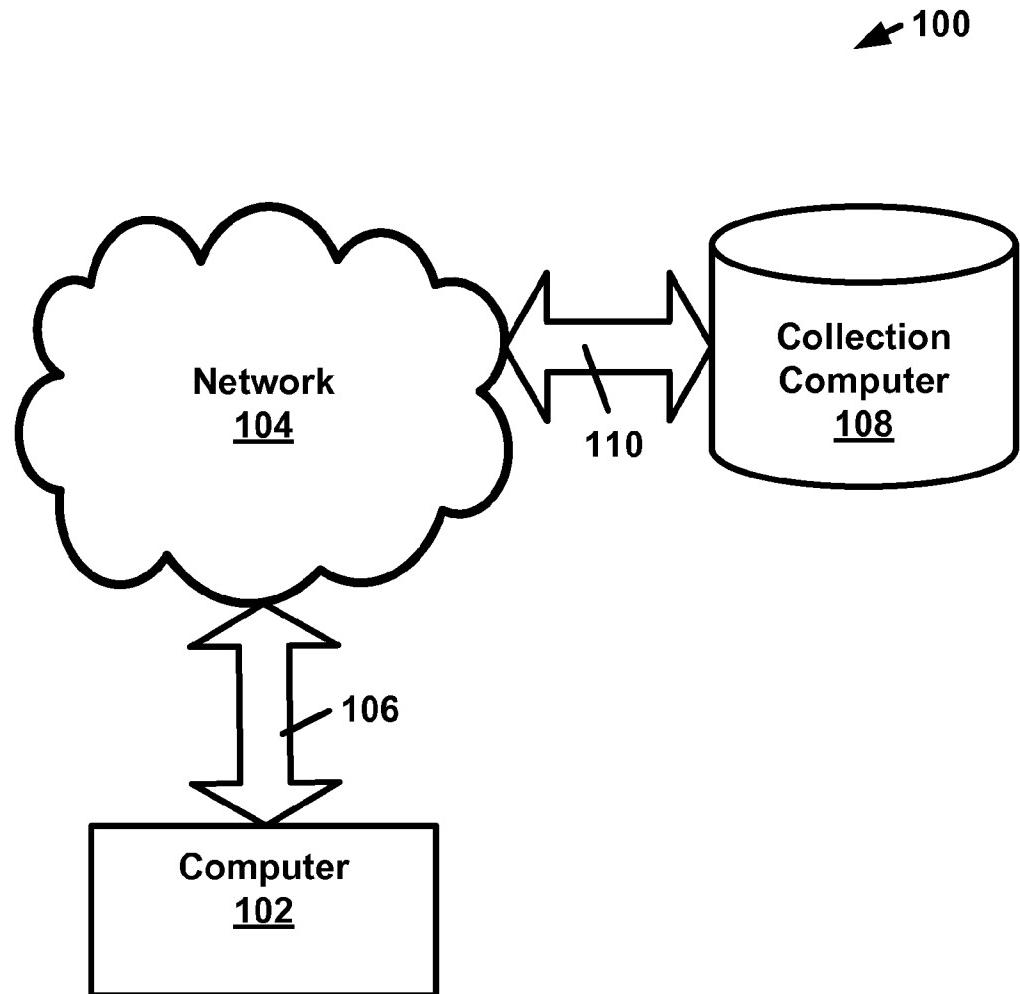


FIG. 1

U.S. Patent

Sep. 16, 2014

Sheet 2 of 12

US 8,839,422 B2

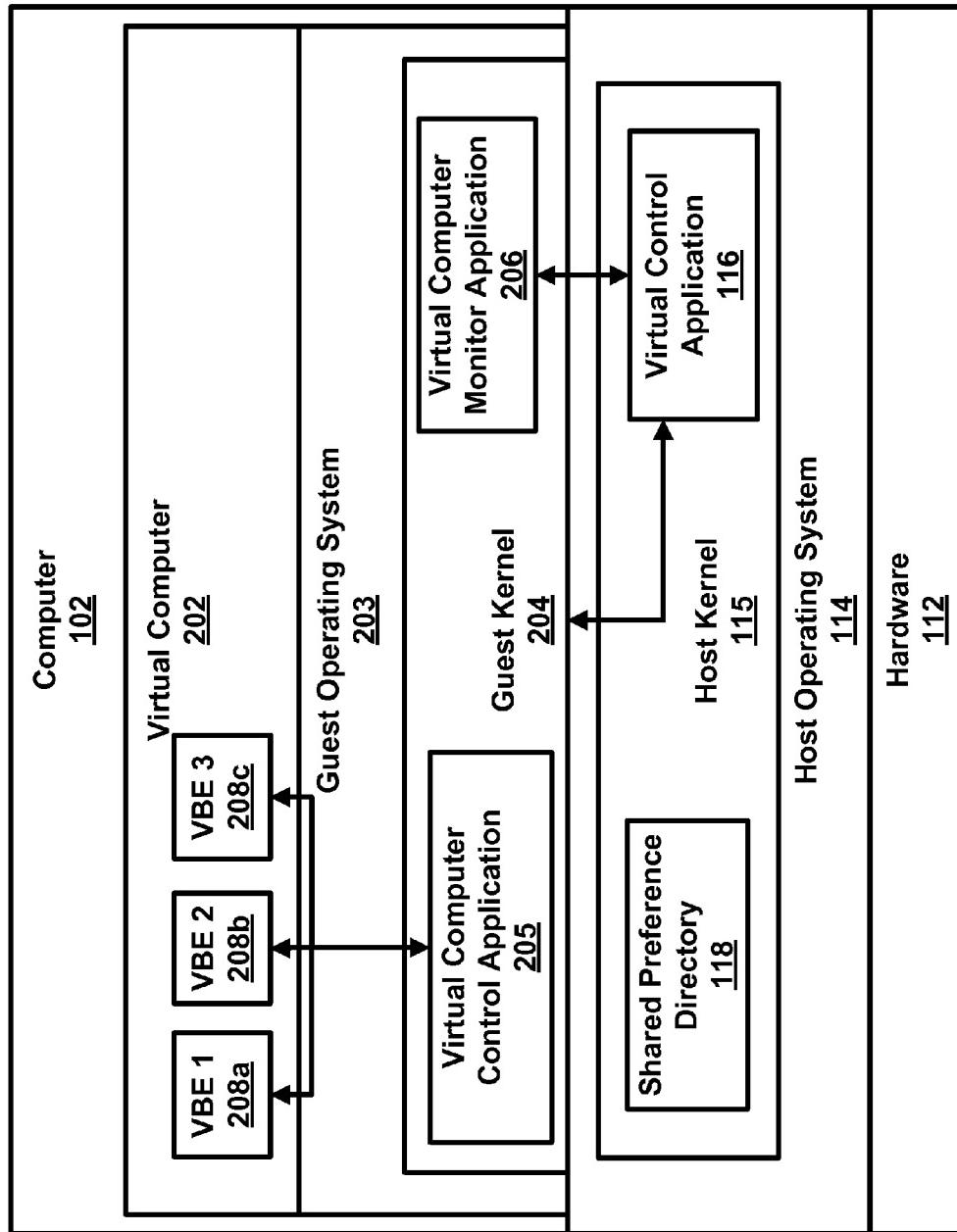


FIG. 2

U.S. Patent

Sep. 16, 2014

Sheet 3 of 12

US 8,839,422 B2

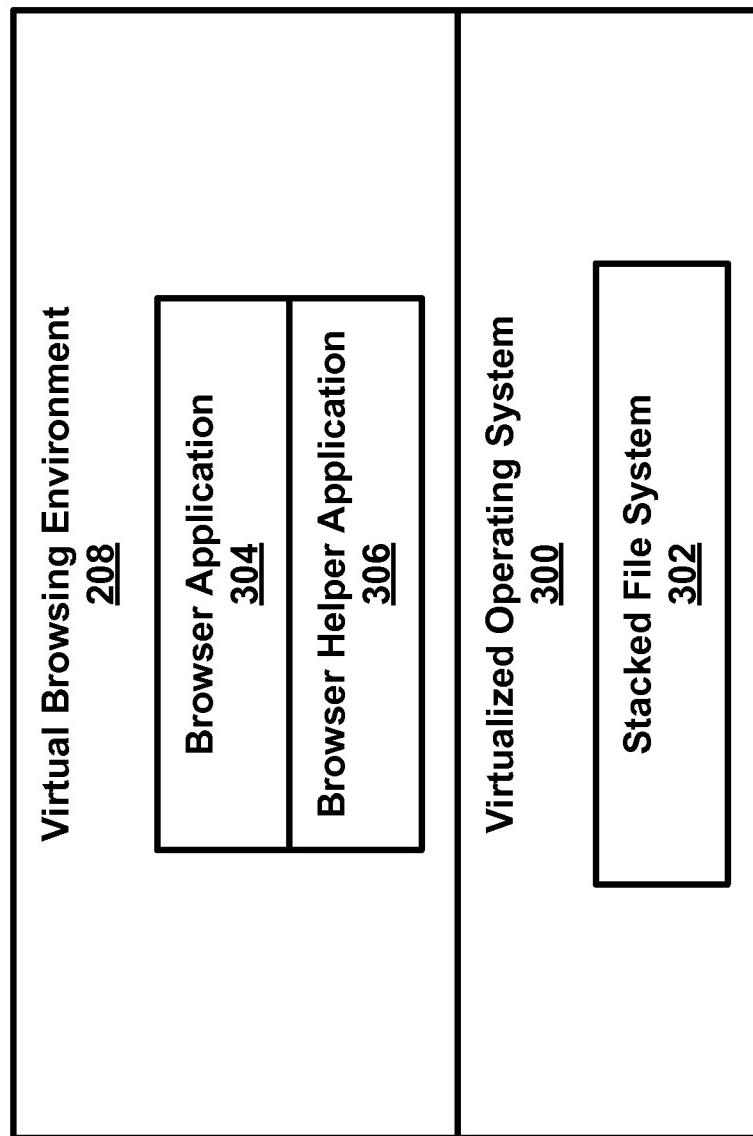


FIG. 3

U.S. Patent

Sep. 16, 2014

Sheet 4 of 12

US 8,839,422 B2

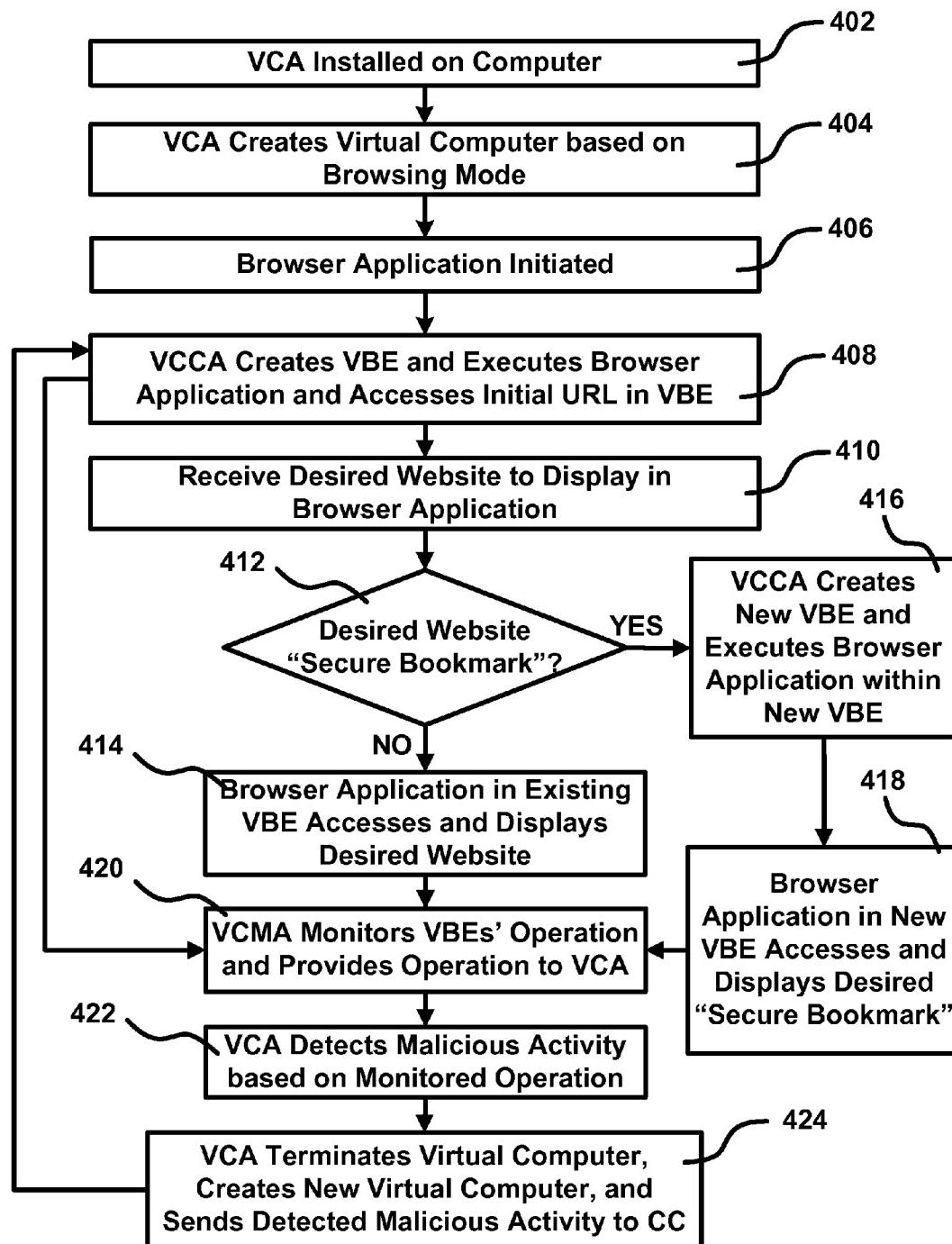


FIG. 4

U.S. Patent

Sep. 16, 2014

Sheet 5 of 12

US 8,839,422 B2

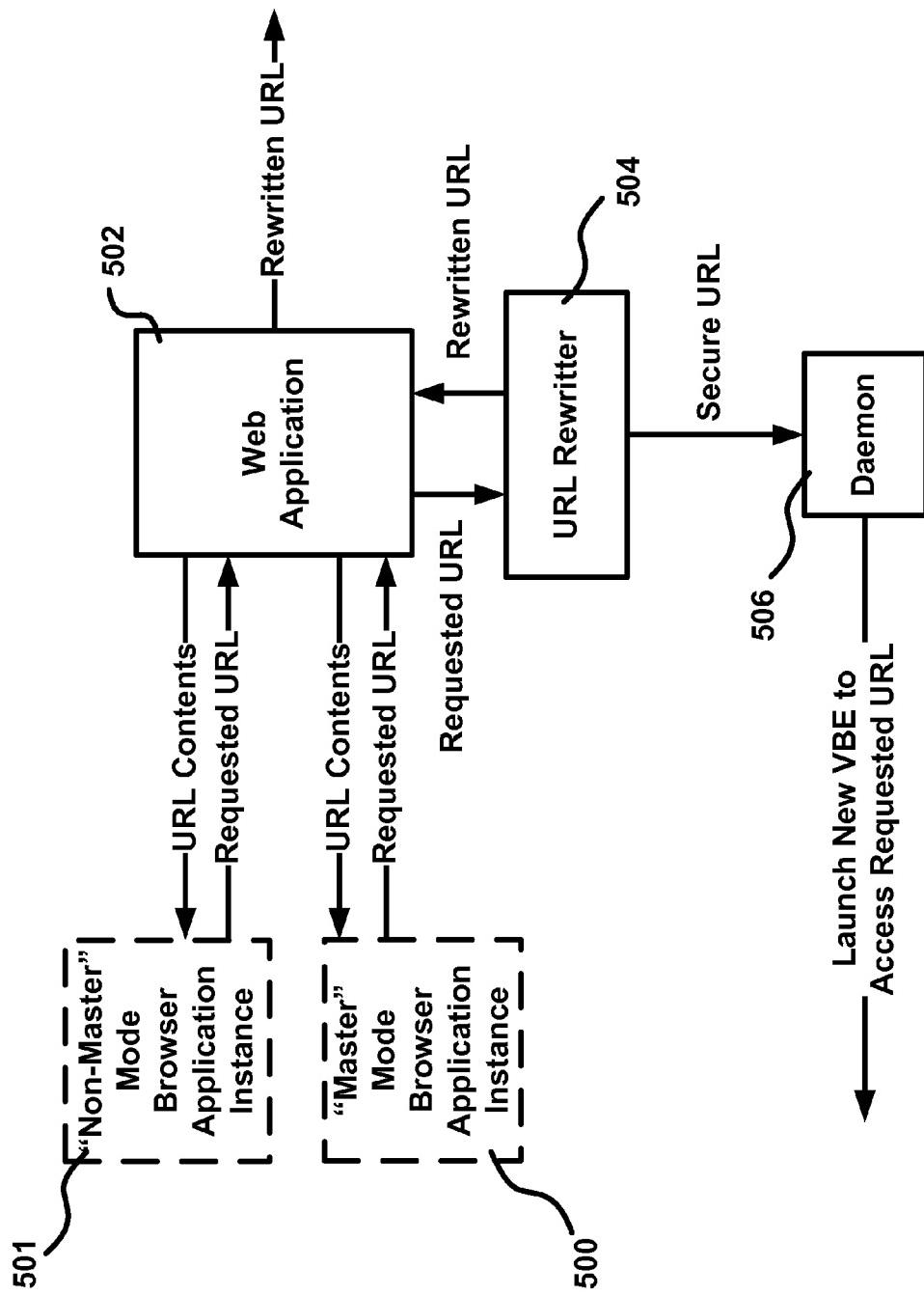


FIG. 5

U.S. Patent

Sep. 16, 2014

Sheet 6 of 12

US 8,839,422 B2

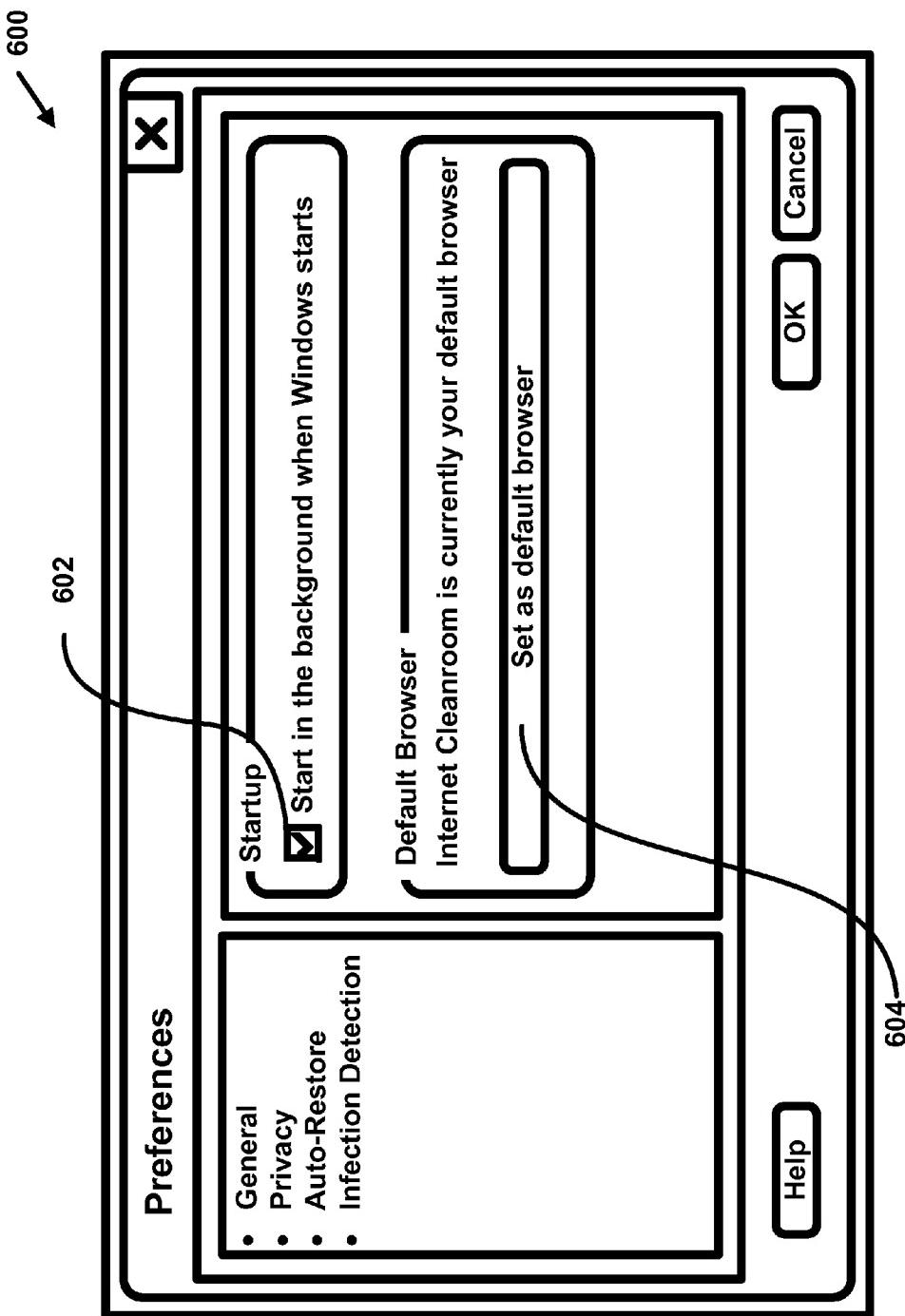


FIG. 6

U.S. Patent

Sep. 16, 2014

Sheet 7 of 12

US 8,839,422 B2

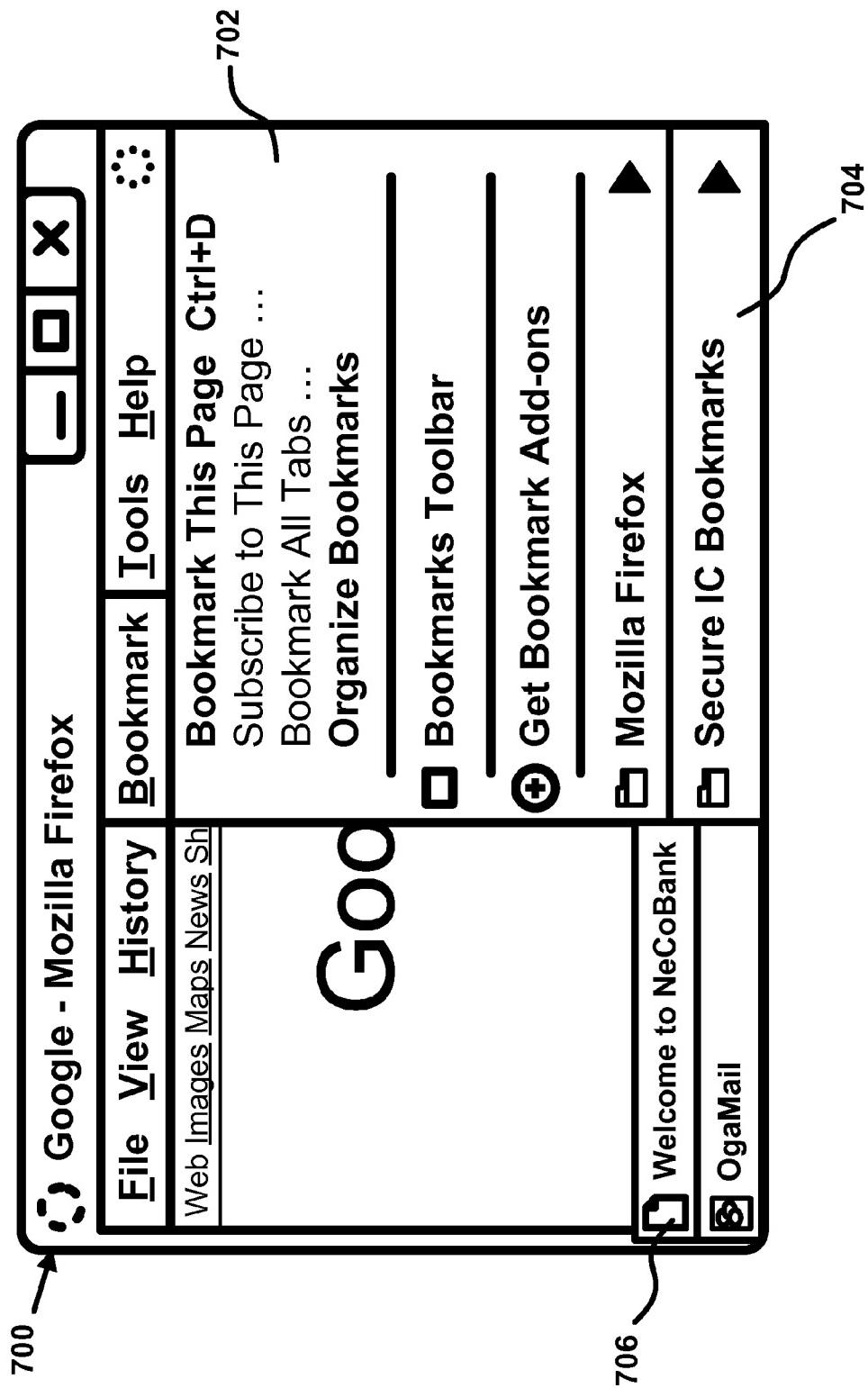


FIG. 7

U.S. Patent

Sep. 16, 2014

Sheet 8 of 12

US 8,839,422 B2

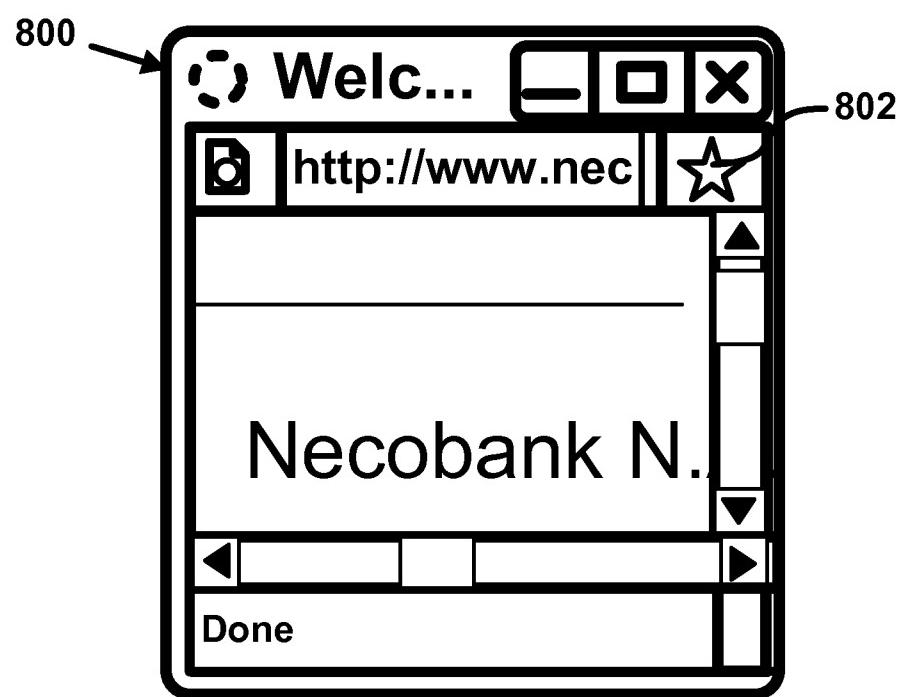


FIG. 8

U.S. Patent

Sep. 16, 2014

Sheet 9 of 12

US 8,839,422 B2

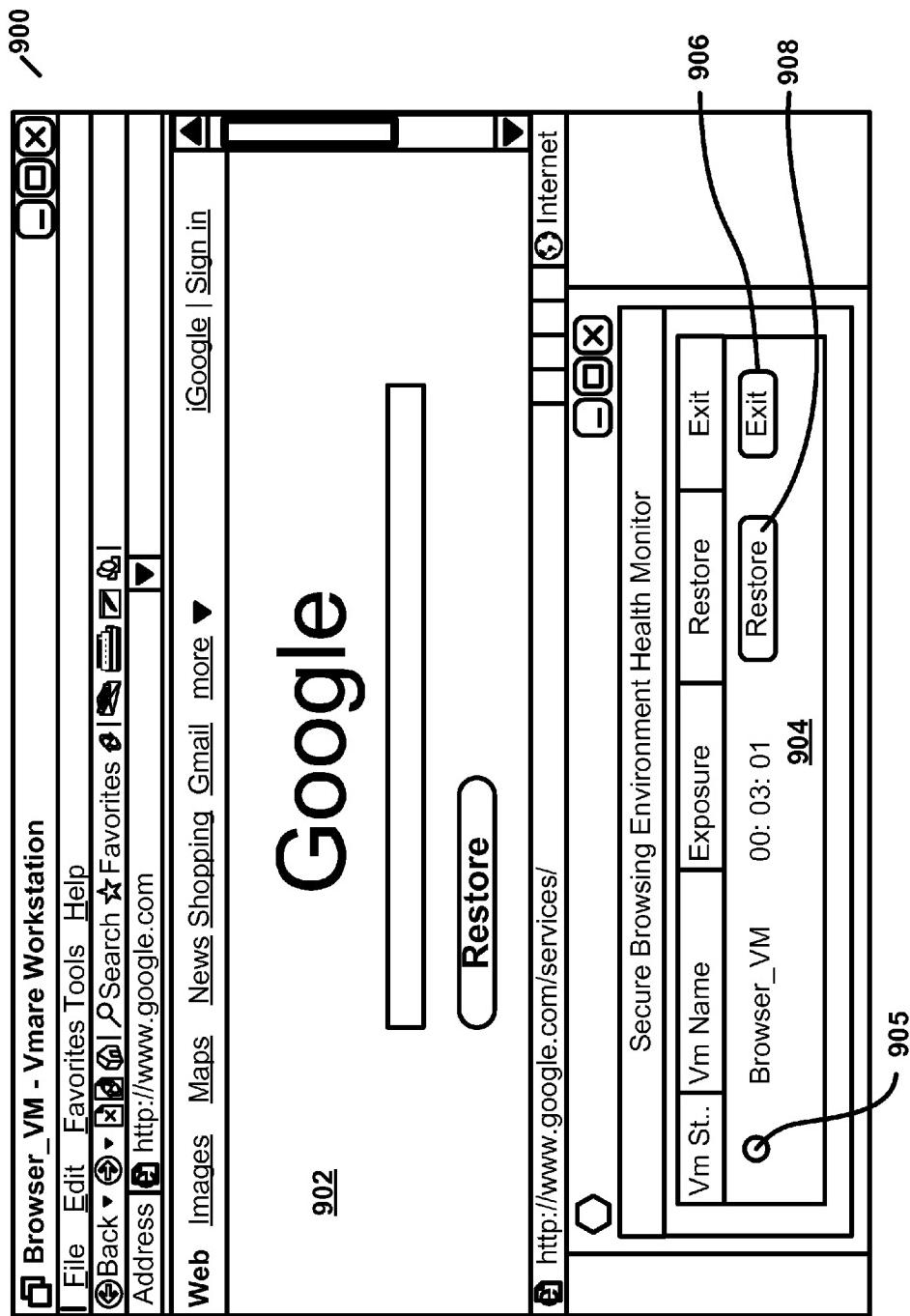


FIG. 9

U.S. Patent

Sep. 16, 2014

Sheet 10 of 12

US 8,839,422 B2

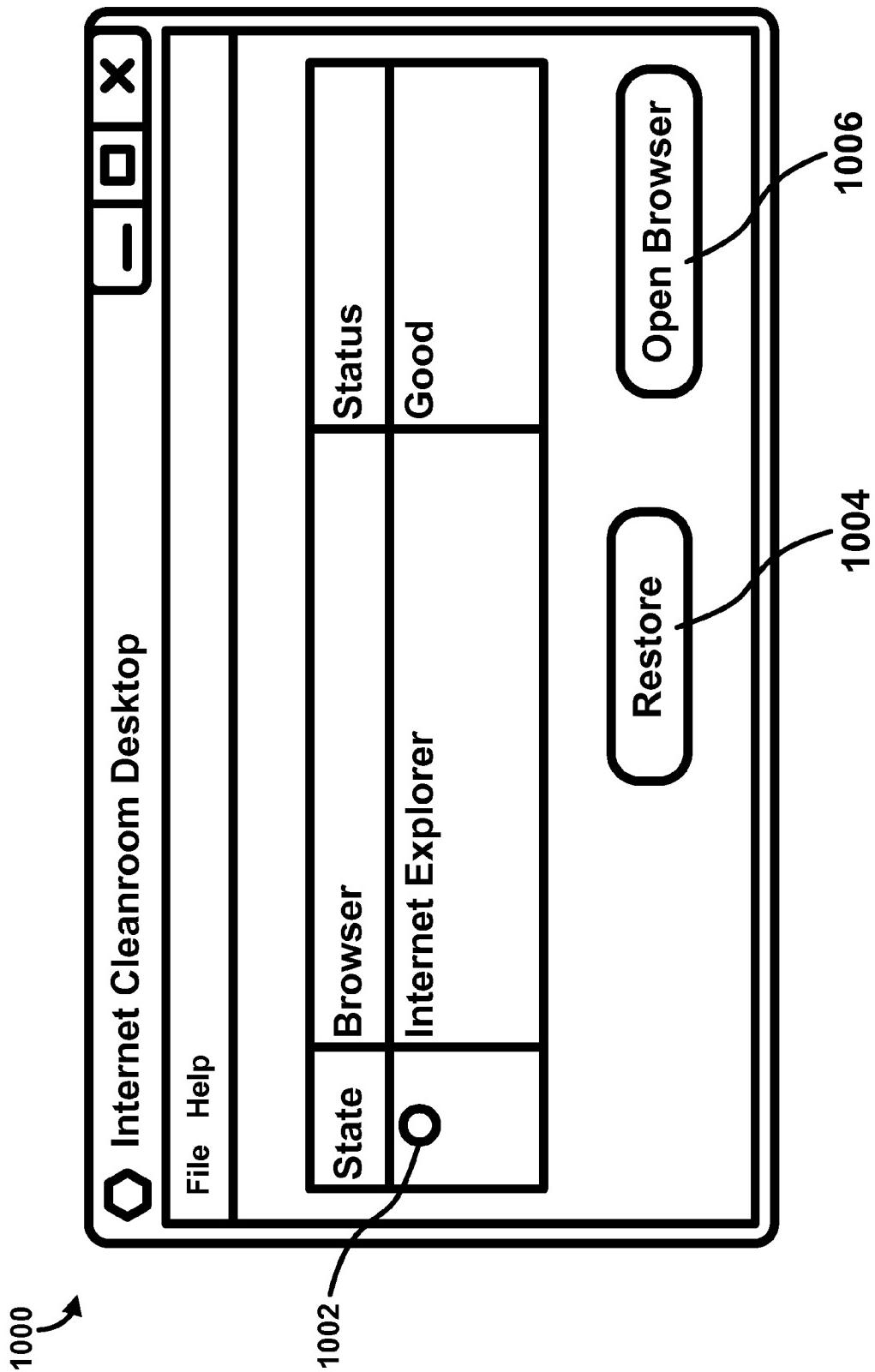


FIG. 10

U.S. Patent

Sep. 16, 2014

Sheet 11 of 12

US 8,839,422 B2

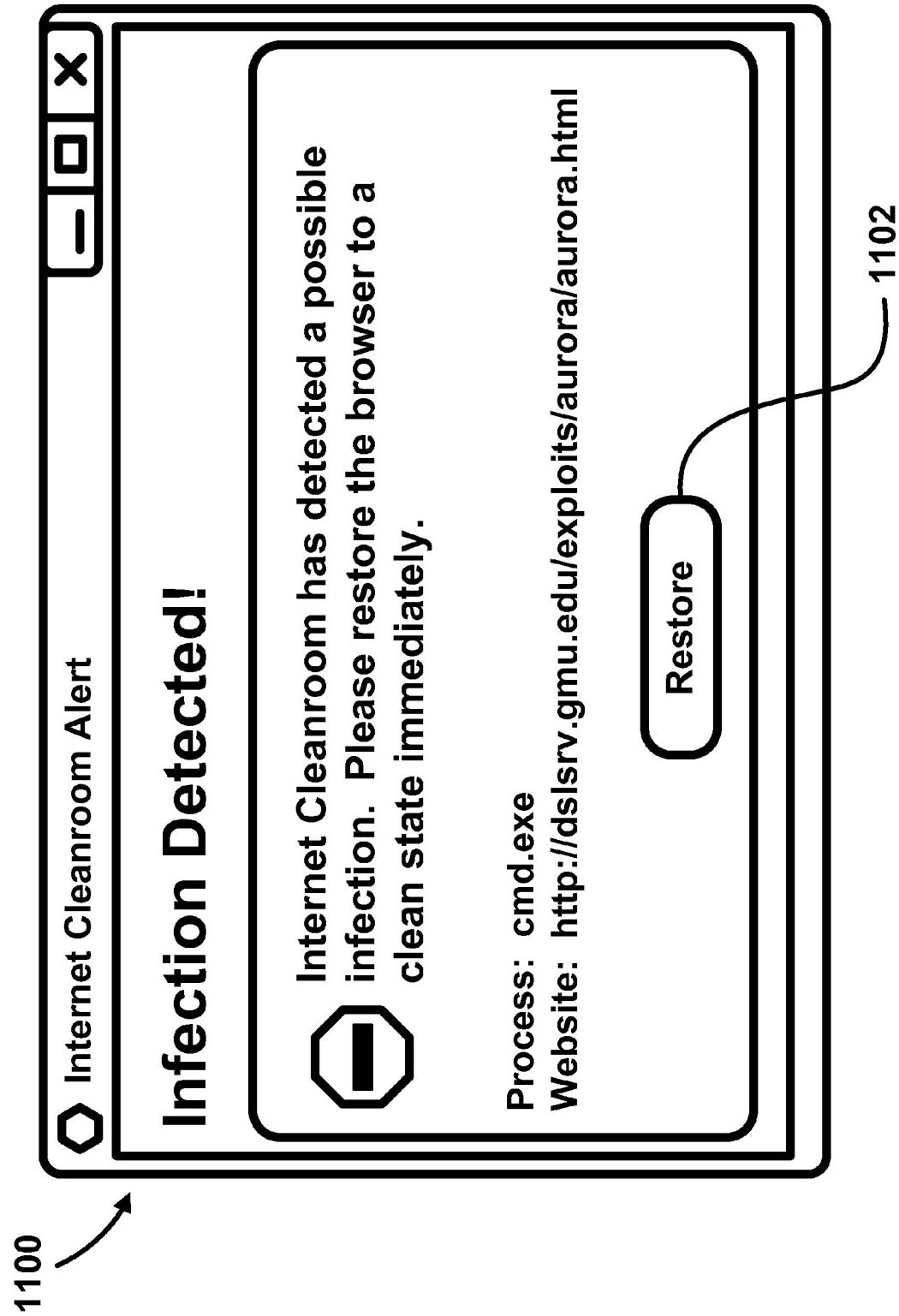


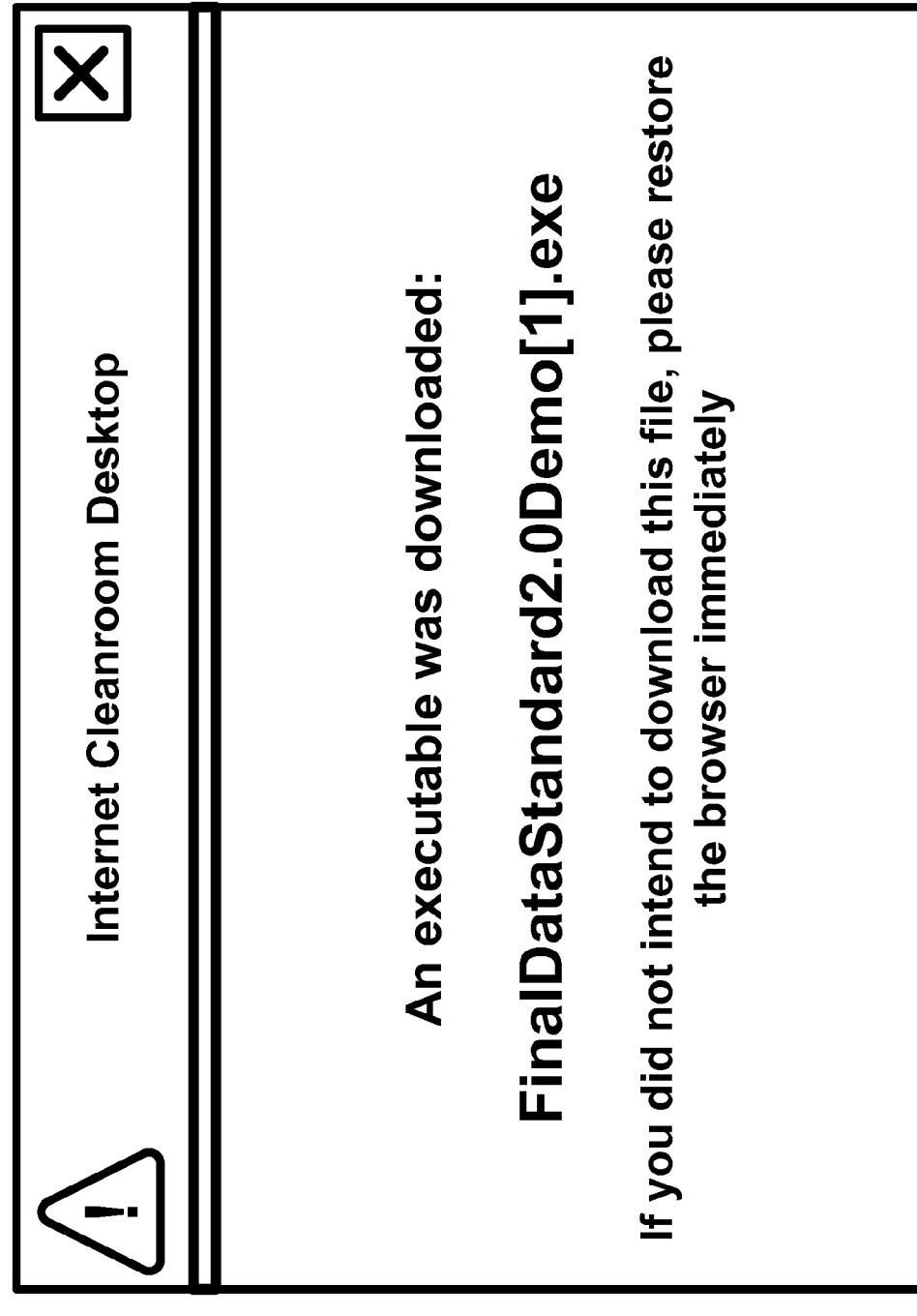
FIG. 11

U.S. Patent

Sep. 16, 2014

Sheet 12 of 12

US 8,839,422 B2



1200

FIG. 12

US 8,839,422 B2

1**VIRTUAL BROWSING ENVIRONMENT****CROSS-REFERENCE TO RELATED APPLICATIONS**

This application claims priority to U.S. Provisional Application No. 61/221,749, filed on Jun. 30, 2009, entitled "Safe-Fox: A Safe Lightweight Virtual Browsing Environment," the entire content of which is hereby incorporated by reference.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

This invention was made with government support under Army contract #W31P4Q-07-C-0244 awarded by Defense Advance Research Projects Agency. The government has certain rights in the invention.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

FIG. 1 illustrates a system for providing a virtual browsing environment according to an aspect of an embodiment of the invention.

FIG. 2 illustrates a computer included in the system of FIG. 1, according to one embodiment of the invention.

FIG. 3 illustrates a virtual browsing environment provided by the computer of FIG. 2, according to an aspect of an embodiment of the invention.

FIG. 4 is a flow chart illustrating a method of providing a virtual browsing environment using the system of FIG. 1, according to an aspect of an embodiment of the invention.

FIG. 5 illustrates a method of determining whether a desired website corresponds to a secure bookmark, according to an aspect of an embodiment of the invention.

FIG. 6 illustrates a user interface that allows a user to select preferences for a virtual browsing environment, according to an aspect of an embodiment of the invention.

FIG. 7 illustrates a user interface that allows a user to select a secure bookmark within a browser application executed within a virtual browsing environment, according to an aspect of an embodiment of the invention.

FIG. 8 illustrates a user interface that displays a secure bookmark within a browser application executed within a virtual browsing environment, according to an aspect of an embodiment of the invention.

FIG. 9 illustrates a user interface that displays a website within a browser application executed within a virtual browsing environment and displays a health monitor for the browser application, according to an aspect of an embodiment of the invention.

FIG. 10 illustrates a user interface that displays a health monitor of a browser application executed within a virtual browsing environment, according to an aspect of an embodiment of the invention.

FIG. 11 and FIG. 12 illustrate user interfaces that display alerts to a user regarding a browser application executed within a virtual browsing environment, according to an aspect of an embodiment of the invention.

DETAILED DESCRIPTION OF EMBODIMENTS

FIG. 1 illustrates a system 100 for providing a virtual browsing environment according to one embodiment of the invention. As described below, embodiments of the system 100 may provide a virtual browsing environment for executing a browser application on a computer. By executing the

2

browser application within a separate virtual browsing environment, other applications, data, and modules of the computer may be protected from any malicious activity associated with the execution of the browser application. In addition, because in some embodiments only the browser application may be executed within the virtual browsing environment, malicious activity associated with the execution of the browser application may be easily detected.

As shown in FIG. 1, the system 100 may include at least one computer 102, at least one network 104, and at least one collection computer ("CC") 108. The computer 102 and the network 104 may be connected by a connection 106, and the network 104 and the collection computer 108 may be connected by a connection 110. The network 104 may include the Internet, a local area network, a wide area network, or combinations thereof. It should be understood that the network 104 may include one or more networks or communication systems, such as the Internet, the telephone system, satellite networks, cable television networks, and various other private and public networks. In addition, the connections 106 and 110 may include wired connections (such as wires, cables, fiber optic lines, etc.), wireless connections, or combinations thereof. Furthermore, although not shown, other computers, systems, devices, and networks may also be connected to the network 104.

With continued reference to FIG. 1, the collection computer 108 may receive data from the network 104 over the connection 110. In some embodiments, the collection computer 108 may also send data to the network 104 or one or more computers or networks. The collection computer 108 may also include hardware, such as one or more memory modules, one or more processors, and one or more input/output modules. In addition, the collection computer 108 may include an operating system to manage the hardware. In some embodiments, the collection computer 108 may also include a database that stores data received from the network 104. The data included in the database may be stored in computer's 108 one or more memory modules, and the data may be managed by a database management application. For example, the collection computer 108 may include a MySQL server running on a L.A.M.P. (Linux, Apache, mySQL, and PHP) stack or other web-based database server systems.

FIG. 2 illustrates the computer 102 of FIG. 1 according to one embodiment of the invention. It should be understood that the computer 102 may include a desktop computer, a laptop computer, a tablet computer, an electronic reading device (e.g., Amazon Kindle), a mobile telephone (e.g., Apple iPhone), a personal data assistant or any other device that may execute software applications. As shown in FIG. 2, the computer 102 may include hardware 112, such as one or more processors, memory modules, input/output modules, or combinations thereof. The one or more input/output modules may communicate with one or more input/output devices connected to the computer 102, such as printers, scanners, monitors, networks (including the network 104), external memory modules, etc. The memory modules may include one or more random-access memories, read-only memories, disks, application specific integrated circuits, programmable read-only memories, or combinations thereof. The memory modules may store data, applications, and combinations thereof. For example, the memory modules may include non-transitory computer readable mediums that store instructions, which perform particular functionality when executed by one or more processors included in the hardware 112. For example, as shown in FIG. 2, the computer 102 may also include a host operating system 114 that provides an interface between the hardware 112 and a user operating the computer 102. The host

US 8,839,422 B2

3

operating system 114 may be stored in the one or more memory modules and may be executed on the one or more processors included in the hardware 112. The host operating system 114 may include a well-known operating system, such as Microsoft Windows, Linux Redhat, UNIX, or Apple MacOs.

The host operating system 114 may include at least one host kernel 115. The host kernel 115 may manage the communication between the hardware 112 and applications executed by the hardware 112. For example, the host kernel 115 may provide inter-application communication, may manage data retrieved from and stored to the one or more memory modules included in the hardware 112 by the applications, and may manage data received from and output to the input/output modules included in the hardware 112.

As shown in FIG. 2, the host kernel 115 may include a virtual control application (“VCA”) 116. As described in more detail below, the host kernel 115 may use the virtual control application 116 to create and manage a virtual computer. Accordingly, the VCA 116 may provide virtualization functionality, such as that provided by Windows VMware workstation or player; Sun Microsystems VirtualBox; Parallels virtualization products, Xen virtualization products, or combinations thereof. The host kernel 115 may also include a shared preference directory 118, which may store preferences for an application, such as a browser application.

It should be understood that the one or more memory modules included in the hardware 112 may store other applications besides those explicitly shown in FIG. 2. In addition, the functionality provided by the applications stored in the one or more memory modules may be combined and distributed in various configurations. For example, the VCA 116 may be combined with other applications or may be distributed among several applications. The one or more memory modules may also store other data used by the host operating system 114 or other applications executed within the computer 102.

In operation, as shown in FIG. 2, the host kernel 115 may execute the VCA 116 to create a virtual computer 202. The virtual computer 202 may include its own guest host operating system 203 with a guest kernel 204. The guest operating system 203 and guest kernel 204 may operate similar to the host operating system 114 and host kernel 115. This type of virtualization where a generally complete copy of an operating system is provided within a virtual computer is generally referred to as “full virtualization.” Outside of the virtual computer 202, the host operating system 114 may continue to interact and manage the hardware 112, while the guest operating system 203 also may interact and manage the hardware 112. Therefore, the virtual computer 202 may create a second, isolated computing environment within the computer 102. Each computing environment may execute different applications, access data from different locations in a memory module or from different memory modules, provide different operating systems, or combinations thereof.

For example, in some embodiments, the host operating system 114 may include a Microsoft Windows operating system (e.g., Windows XP, Vista, 7) and the guest operating system 203 may include a Linux operating system (e.g., Redhat Enterprise Linux 5.3). Therefore, while the host operating system 114 may only execute applications designed for a Windows operating system, the guest operating system 203 may execute applications designed for a Linux operating system. In this situation, the shared preference directory 118 may be a Windows file but may be mapped to a Linux file or directory, which allows the guest operating system 203 to

4

access and manipulate the shared preference directory 118 although it is part of the generally non-compatible host operating system 114.

As mentioned above, creating the virtual computer 202 may provide isolation between computing performed within the virtual computer 202 and computing performed outside the virtual computer 202 through the host operating system 114. For example, the virtual computer 202 may be unaware of any computing performed outside of the virtual computer 202. Accordingly, an application executed within the virtual computer 202 generally cannot access an application executed outside the virtual computer 202. For example, in some embodiments, the only portion of the host operating system 114 visible to and accessible by the guest operating system 203 is the shared preference directory 118. Therefore, the guest operating system 203 may not access or modify the host operating system 114 except for the shared preference directory 118. This restriction may limit the access of a malicious or compromised guest operating system 203 to only the shared directory and may prevent any malicious activity occurring within the virtual computer 202 from compromising the host operating system 114 and infecting the entire computer 102.

As shown in FIG. 2, the guest kernel 204 may include a virtual computer control application (“VCCA”) 205 and a virtual computer monitor application (“VCMA”) 206. The VCCA 205 may manage the operation of the virtual computer 202. For example, as shown in FIG. 2, the VCCA 205 may create one or more virtual browsing environments (“VBEs”) 208 (e.g., VBE 1 208a, VBE 2 208b, and VBE 3 208c). Once created, the VCMA 206 may monitor the operation of each VBE 208 and may report each VBE’s operation to the VCA 116. To create a VBE 208, the VCCA 205 may use one or more virtualization modules or applications, such as OpenVZ, UnionFS patches, Solaris Zones, BSD Jail, or combinations thereof.

FIG. 3 illustrates a VBE 208 according to one embodiment of the invention. As shown in FIG. 3, the VBE 208 may include a virtualized operating system 300 (e.g., CentOS Linux 5.3). Rather than including a complete operating system with a kernel, the virtualized operating system 300 may share the guest kernel 204 of the guest operating system 203. Creating a virtual environment that shares a kernel from another operating system is often referred to as “lightweight” virtualization. Lightweight virtual environments generally operate like full virtual environments (e.g., the virtual computer 202), but generally require less overhead due to the shared kernel. However, because the VBE 208 and the virtual computer 202 share the same kernel (i.e., the guest kernel 203), in some embodiments, the VBE 208 generally executes the same or a version of the same operating system as the virtual computer 202.

Each VBE 208 may execute a browser application 304. In some embodiments, the browser application 304 may be stored in the one or more memory modules included in the hardware 112 and may be executed by the one or more processors included in the hardware 112. The browser application 304 may send and receive data from the network 104 and may present at least received data to a user. For example, the browser application 304 may be used to access a website available over the network 104 (e.g., the Internet) and display the contents of the website to a user. The browser application 304 may include a well-known browser application, such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, or Apple Safari. The preferences stored in the shared preference directory 118 for the browsing application may include browsing history, bookmarks, secure bookmarks (as

US 8,839,422 B2

5

described below with respect to FIG. 4), cookies, passwords, add-ons, personal information, etc.

In some embodiments, configuration files of the browser application 340 may be modified. For example, the browser application 340 may be configured to use a specific proxy, such as the web application 502 described below with respect to FIG. 5. In addition, as also described below, in some embodiments, the browser application 340 may be executed in different modes and each mode may be configured differently. For example, in some modes, the browser application 340 may be configured to import user preferences stored in the shared preference directory 118 and in another mode the browser application 340 may be configured to operate without importing user preferences from the shared preference directory 118.

In some embodiments, each VBE 208 may be assigned its own process namespace, internet protocol (“IP”) address, and file system. For example, as shown in FIG. 3, the virtualized operating system 300 may include a stacked file system 302. The stacked file system 302 may provide a file system accessible by applications executed within the VBE 208 (e.g., the browser application 304). The whitepaper titled “Efficiently Tracking Application Interactions using Lightweight Virtualization” authored by Yih Huang, Angelos Stavrou, Anup K. Ghosh, and Sushil Jajodia, the entire contents of which is herein incorporated by reference, describes a method of creating a stacked file system for lightweight virtual environments. As described in this whitepaper, initially, a read-only template of a VBE 208 may be created (e.g., upon installation of the VCA 116, the VCCA 205, or combinations thereof). The read-only template may include a copy of any data and applications that will be executed within the VBE 208. In some embodiments, rather than creating a separate physical copy of the data and applications, the read-only template may only include a mapping to the data and applications already stored in the computer’s 102 hardware 112. For example, the read-only template may include a copy of or a mapping to the binary code and libraries for the browser application 304.

When a VBE 208 is created, a daemon or application (e.g., a Perl script) included in the VCCA 205 may construct a new stacked file system for the new VBE 208 by creating a writeable copy of the read-only template (i.e., a writable layer). In some embodiments, the daemon may use UnionFS functionality to create the stacked file system. The writable layer may be associated with the newly-created VBE 208 and may be mounted as the root of the file system for the new VBE 208. As mentioned above, rather than including separate physical copies of the data and applications included in the read-only template, the writable layer may include mappings to the copied data and applications. This mapping further may reduce the amount of memory needed even when multiple VBEs 208 are created.

The application included in the VCCA 205 may also allocate to each new VBE 208 an IP address. As described in detail below, in some embodiments, the browser application 304 executed with in a VBE 208 may be executed in various browsing modes. Depending on the browsing mode of the browser application 304 to be executed within the new VBE 208, the VCCA 205 may modify the creation of the new VBE 208. For example, when a new VBE 208 is created for a master mode browser application 304, the VCCA 205 may assign the new VBE 208 a predetermined fixed IP address. However, when the VCCA 205 creates new VBEs 208 in other operating modes, the VCCA 205 can dynamically assign IP addresses to the new VBEs 208. A new VBE 208 can use the domain name server (“DNS”) table from the guest

6

operating system 203, or a new VBE 208 can use an arbitrary “trusted” DNS service, such as Open DNS, to provide additional security.

After assigning a new VBE 208 an IP address, the application within the VCCA 205 can boot up the new VBE 208, execute the browser application 304 within the VBE 208, and project the browser application 304 window or output to a display output of the computer 102. In some embodiments, the application within the VCCA 205 that creates new VBEs 10 208 can be associated with the browser application 304 (e.g., with an icon or program selection accessible by a user to initiate the browser application 304) so that execution of the browser application 304 triggers the execution of the application.

15 After a new VBE 208 is created and an application is executed with the VBE 208 (e.g., the browser application 304), if the application wants to write data to its stacked file system 302, a copy-on-write (“COW”) operation within the stacked file system 302 can create a new version of the file in 20 the writable layer. This new version of the file can then be used by the VBE 208 for later reads and writes of that particular file. Accordingly, although VBEs 208 can start in generally the same state as the read-only file template (except for an IP address), the stacked file systems 302 of each VBE 208 can drift apart over time as applications executed within each VBE 208 modify their respective stacked file systems 302.

25 With continued reference to FIG. 3, the VBE 208 may execute the browser application 304. In some embodiments, depending on a browsing mode set for the VBE 208, the VCCA 205 may load preferences into the browser application 304 from the shared preference directory 118. The browser application 340, the VBE 208, the VCCA 205, or combinations thereof may also update or store preferences to the shared preference directory 118 based on the operation of the browser application 304 (e.g., if a user adds a new bookmark or accesses a new website).

30 As shown in FIG. 3, the browser application 304 may include or be associated with a browser helper application 306. The browser helper application 306 may be stored in one or more memory modules included in the hardware 112 and may be executed by one or more processors included in the hardware 112. In some embodiments, the browser helper application 306 may be stored as part of the browser application 304, as a separate application, or a combination thereof. As described below with respect to FIG. 4, the browser helper application 306 may monitor the operation of the browser application 304 and may provide information about the application’s operation to the VCMA 206. For example, the browser helper application 306 may record websites accessed by the browser application 304, data downloaded by the browser application 304, data stored in the stacked file system 302 by the browser application 304, applications executed by the browser application 304, inter-process communications between the browser application 304 other applications executed within the computer 102, the virtual computer 202, or the VBE 208, and any attempts to do any of the foregoing.

35 It should be understood that in some embodiments the virtual computer 102 is not needed and the one or more VBEs 208 may be directly created by the host operating system 114. For example, in some embodiments, the VCA 116 may include the functionality of the VCCA 205 and the VCMA 206 and may be executed by the host kernel 114 of the host 40 operating system 115 to create one or more VBEs 208 directly within the computer 102. Rather than sharing the guest kernel 204 as described above, the VBEs 208 created directly within

US 8,839,422 B2

7

the computer 102 may share the host kernel 115. For example, in some embodiments, the virtual computer 202 may be used to create a Linux virtual computing environment within a Windows-based operating system. The Linux virtual computing environment allows Linux-based light virtualization to be performed to create and manage the VBEs 208. However, if the host operating system 114 of the computer 102 is a Linux operating system, the virtual computer may be eliminated because the Linux-based light virtualization may be directly performed by the Linux host operating system. In addition, if Windows-based light virtualization is instead used to create and manage the VBEs 208 and the host operating system 114 is Windows-based, no separate virtual computer may be needed in order to use the Windows-based lightweight virtualization. In this regard, the virtual computer 202 may be used whenever the virtualization used to create the VBEs 208 is not supported by the host operating system 114 of the computer 102.

Accordingly, as used throughout the present specification, a VBE 208 may be described as sharing the kernel from the operating system “supporting” the VBE 208. Therefore, when a VBE 208 is created within the virtual computer 202, the guest operating system 203 may “support” the VBE 208 and the VBE 208, therefore, may share the guest kernel 204 of the “supporting” guest operating system 203. Similarly, when a VBE 208 is created directly within the computer 102, the host operating system 114 may “support” the VBE 208 and the VBE 208, therefore, may share the host kernel 115 of the “supporting” host operating system 114.

FIG. 4 illustrates a method of providing a virtual browsing environment performed by the system 100 according to one embodiment of the invention. It should be understood that the method illustrated in FIG. 4 may include more or less steps than those illustrated. The illustrated method may also be distributed among multiple methods or may be included as part of a larger method. Also, the method of FIG. 4 should not be construed as limiting the order, number, omission, addition, or other variation of the individual steps illustrated. As shown in FIG. 4, the VCA 116 may be initially installed on the computer 102 (at 402). It should be understood that the VCA 116 may be installed on the computer 102 from a computer-readable medium, such as a disk or drive, or over a network, such as the network 104. In some embodiments, when the VCA 116 is installed, a browsing mode may be set. For example, the browsing mode may be set to a master mode, a secure-bookmark mode, or a private mode. In some embodiments, a user may be prompted to set the browsing mode by selecting preferences upon installation or initiation of the VCA 116 (e.g., using a selection mechanism, such as a check box, a button, a toggle box, a drop-down menu, etc.). The VCA 116 may also include a default browsing mode that may be used if a user does not specify a particular browsing mode.

Once the VCA 116 is installed, the VCA 116 creates the virtual computer 202 based on the browsing mode (at 404). As described above with respect to FIG. 2, the virtual computer 202 may include the guest operating system 203, the guest kernel 204, the VCCA 205, and the VCMA 206, or combinations thereof. As also described above, in some embodiments, the guest operating system 203 may be different from the host operating system 114 of the computer 102. For example, the host operating system 114 may include a Microsoft Windows-based operating system and the guest operating system 203 may include a Linux-based operating system.

In some embodiments, the VCA 116 may create the virtual computer 202 upon boot-up of the computer 102. The VCA 116 may also create or build a “snapshot” of the virtual computer 202 upon its boot-up or initiation. The “snapshot”

8

may be based on the read-only template included in the virtual computer 202, as described above. “Snapshots” are well-known in the computer industry and may be used to capture particular information about a currently-executing application, which may allow the application to be quickly restored to the captured state at a later point without having to restart the application from scratch. The UnionFS file system service for Linux may provide snapshot functionality. Accordingly, the VCA 116 may use the “snapshot” of the virtual computer 202 to quickly restart the virtual computer 202 at a later time, such as after it is terminated due to the detection of malicious activity (described below). It should be understood that if the one or more VBEs 208 are created directly in the computer 102 as described above, there may be no need to create the virtual computer 202 at 404.

After the virtual computer 202 is created and a browser application 304 is initiated (e.g., by a user or by another application) (at 406), the VCCA 205 may create a VBE 208, execute the browser application 304 within the VBE 208, and access an initial URL with the browser application 304 (at 408). In some embodiments, upon the VBE’s 208 creation, the VCA 116 may capture a “snapshot” of a VBE 208. The “snapshot” may capture the VBE 208 with a “pristine” operating system before any potential malicious activity has occurred based on the user’s operation of the browser application 304 within the VBE 208. As described above, a “snapshot” may be used to quickly restore an application to the captured state without having to completely restart the application from scratch. Therefore, the “snapshot” may allow the VCA 116 to quickly restore or create a new VBE 208, such as after a previous VBE 208 was terminated due to the detection of malicious activity (described below). It should be understood that the “snapshot” of the virtual computer 202 and the “snapshot” of the “pristine” VBE 208 may be combined in a single “snapshot.” Additionally, if a virtual computer 202 is not used, the VCA 116 may just take a “snapshot” of the “pristine” VBE 208.

In some embodiments, the functionality of the browser application 304 executed within the VBE 304 may be modified based on a browsing mode. For example, if a browsing mode is set to a “master” mode, the browser application 304 executed within the VBE 208 may support many typical functions of a browser application 304 running directly on the computer 102. Accordingly, the browser application 304 may be imported with browsing preferences from the shared preference directory 118, such as browsing history, cookies, passwords, bookmarks, personal information, etc. In “master” mode, the browser application 304 may also store preferences to the shared preference directory 118, such as browsing history, bookmarks, cookies, passwords, add-ons, etc.

If the browsing mode is set to a “private” mode, the browser application 304 may be executed within the VBE 208 without importing any preferences from the shared preference directory 118 and without storing any new preferences to the shared preference directory 118. Therefore, the browser application 304 may be initiated and executed in an “anonymous” state where generally no personal data about the user interacting with the browser application 304 is accessible by the browser application 304. In some embodiments, a user may execute a browser application 304 in a “private mode” by selecting an icon or a program associated with separate browser application 304 configured to operate only in a “private mode.” In other embodiments, an icon may be included and displayed within the browser application 340 that a user may click or select in order to activate an instance of the browser application 340 in “private mode.” The new “private mode” instance may be included in or take the place of the

US 8,839,422 B2

9

current browser application 340 instance, may be created as a separate instance from the current browser application 340, or both.

If the browsing mode is set to a “secure-bookmark” mode, the functionality of the browser application 304 may be limited to accessing and interacting with a “secure bookmark.” For example, as mentioned above, the shared preference directory 118 may store uniform resource locators (“URLs”) associated with pre-configured websites specified as “secure bookmarks.” A user may set a website where he or she interacts with (e.g., provides, retrieves, views, etc.) secure information (e.g., an online banking website), as a “secure bookmark.” In some embodiments, a user may use a selection mechanism, such as a button or icon, a drop-down menu, or a check box, to set a website currently displayed in a browser application 304 as a “secure bookmark.” The user may also type the URL of a website into a secure bookmark management interface, similar to bookmark management interfaces typically provided in browser applications, to set a particular URL as a “secure bookmark.”

When the browser application 304 is executed in the “secure-bookmark” mode, the navigation tools of the browser application (e.g., the address line, a bookmark drop-down menu, a history menu, a previous and next selection mechanism, etc.) may be set to read-only, disabled, or removed from the browser application 304, which prevents a user from redirecting the browser application 304 to a different website. In some embodiments, the “secure-bookmark” mode browser application 304 may also be programmed to only access a predetermined set of websites (e.g., based on the “secure bookmark” website’s per-service information and policy), which prevents the user from clicking on a link within a “secure bookmark” website and redirecting the browser application 304 to another (potentially un-secure) website. By limiting the functionality of the browser application, the “secure-bookmark” mode may provide enhanced security for accessing sensitive websites. For example, a user may use the “secure-bookmark” mode when performing secure transactions, such as online banking and shopping. The limited functionality of the browser application 304 may also prevent other browser instances or other websites from spying or interfering with the user’s transactions. In addition, in some embodiments, a separate directory in the shared preference directory 118 may be created (e.g., by the browser application 304; the VBE 208; the VCCA 205, such as a daemon or application executed within the VCCA 205; the VCA 116; or combinations thereof) and associated with each web site designated as a “secure bookmark.” The separate directory may store preferences and other metadata associated with each “secure bookmark” website, such as passwords, account numbers, usernames, etc. In some embodiments, each separate directory may only be accessed when the browser application 304 is operated in a “secure-bookmark” mode and when the browser application is accessing the “secure bookmark” associated with the separate directory.

The browser application’s download and upload functionality may also be limited to provide enhanced computer security in one or all of the browsing modes described above. For example, in a “private” mode, the browser application 304 may prohibit all file uploads or downloads. Similarly, in a “master” or “secure-bookmark” mode, the browser application 304 may allow downloads and/or uploads but may restrict the type or storage location of files uploaded and/or downloaded. For example, in a “master” mode or “secure-bookmark” mode, the browser application 304 may prevent any executable files from being uploaded or downloaded and

10

may limit file downloads or uploads to non-system file folders or location, non-program file folders or location, and/or the “desktop” file folder.

The number of instances of each mode of the browser application that may be executing at the same time on the computer 102 or within the virtual computer 202 may be limited. For example, in some embodiments, there may be only one instance of a “master” mode browser application 304 running at one time. Therefore, if a user initiates a “master” mode browser application 304 (e.g., clicks on an icon associated with the browser application 304) while a “master” mode browser application 304 is already running, a new tab may be opened within the running “master” mode browser application 304 rather than initiating another execution thread or process of the browser application 304. In contrast, in some embodiments, a user may initiate multiple “private” mode browser applications or “secure-bookmark” mode browser applications, and each “private” or “secure-bookmark” mode browser application 304 may be initiated and executed within a separate VBE 208. Each browser application mode may be visually distinguishable from the other modes in order to identify the browsing mode of a particular browser application to a user.

In some embodiments, the browsing mode may be based on how the browser application 304 is initiated on the computer 102. For example, if a user or another application initiates the browser application 304 with a specified initial URL (e.g., by clicking on a website link within an electronic document displayed by the computer 102, selecting a save website shortcut stored on the computer 102, etc.), the VCCA 205 may decide a browsing mode based on whether the specified URL corresponds to a “secure bookmark.” If the specified URL corresponds to a “secure bookmark,” the VCCA 205 may execute the browser application 304 in a “secure-bookmark” mode and may access the specified initial URL. If the specified URL does not correspond to a “secure bookmark,” the VCCA 205 may execute the browser application 304 in either a “master” mode or a “private” mode (e.g., depending on which mode as been specified by a user or is set as a default mode) and may access the specified initial URL. Alternatively, if a user or another application initiates the browser application 304 without specifying a particular initial URL (e.g., by clicking on a browser application icon on the desktop of the computer 102), the VCCA 205 may execute the browser application 304 in either a “master” mode or a “private” mode (e.g., depending on which mode as been previously selected by a user or is set as a default mode) and may access an initial default or “home” URL.

Returning to FIG. 4, after the browser application 304 is executed within the VBE 208 and the browser application 304 accesses the initial URL (either a specified initial URL or a default or “home” URL) (at 408), the VCMA 206 may monitor the VBE’s behavior and provides information about the VBE’s behavior to the VCA 116 (at 420). This functionality is described in detail below. However, as shown in FIG. 4, after the browser application 304 accesses the initial URL (at 408), the browser application 304 may receive a desired website to access and display (at 410). For example, after an initial website is displayed, a user may specify a desired website in various ways, such as by typing a URL in an address line of the browser application 304, clicking on a link within the currently displayed website in the browser application 304, or selecting a website from a drop-down menu (e.g., a favorites menu, a history menu, etc.) (e.g., see FIG. 7). When a desired website is specified, the VCCA 205 may determine whether the desired website corresponds to a “secure bookmark” (at 412).

US 8,839,422 B2

11

In some embodiments, the VCCA 205 may determine whether the desired website corresponds to a “secure bookmark” by comparing the specified desired website to a file of URLs previously set as “secure bookmarks.” For example, as described above, the shared preference directory 118 may store URLs associated with pre-configured websites specified as “secure bookmarks.” If the desired website does not correspond to a URL specified in the shared preference directory 118 as a “secure bookmark” (at 412), the browser application 304 in the existing VBE 208 may access and display the desired website (at 414).

If, however, the desired website corresponds to a URL specified in the shared preference directory 118 as a “secure bookmark” (at 412), the VCCA 205 may create a new VBE 208 and may execute the browser application 304 within the new VBE 208 (at 416). As described above, the VBE 208 may execute the browser application 304 in a “secure-bookmark” mode, which modifies the navigation tools of the browser application 304 and access a separate directory in the shared preference directory 118 that stores preferences and other metadata associated with the desired “secure bookmark.” Once the VBE 208 executes the browser application 304 within the new VBE 208, the browser application 304 may access and display the desired “secure bookmark” (at 418).

FIG. 5 illustrates in more detail a process for determining whether a desired website corresponds to a “secure bookmark” according to one embodiment of the invention. As shown in FIG. 5, instances of the browser application 304 (e.g., a “master” mode browser application instance 500 and a “non-master” mode browser application instance 501) may generate URL requests. In some embodiments, however, a secure bookmark may only be specified from within a master mode browser application instance. For example, in a “private” mode, no browsing preferences, such as any previously-specified “secure bookmarks” may be imported into the browser application instance. Similarly, in a “secure-bookmark” mode, the navigation tools of the browser application may be disabled, which includes the ability to enter a new URL in the address line or choose a website from a menu of bookmarks or secure bookmarks. Accordingly, as shown in FIG. 5, URL requests from browser application instances may be categorized as either requests from “master” mode browser application instances, which may include requests to access a “secure bookmark,” and requests from “non-master” mode browser application instances, which generally cannot include requests to access “secure bookmark.”

As shown in FIG. 5, the browser application instances 500 and 501 may interact with a web application 502 (e.g., a Squib web proxy). In some embodiments, the web application 502 may be included in the VCCA 205. Transmission control protocol (“TCP”) connections not using the proper web application 502 port (e.g., port 3128) may be blocked by one or more firewalls provided by the host or supporting operating system, which may be inaccessible and invisible for processes executing inside the VBEs 208. In some embodiments, if the proxy settings of an instance of the browser application 304 are modified, either by a user or by another application (e.g., malware), the browser application instance may be blocked from reaching the network 104.

The web application 502 may support a feature called URL-rewrite. When this feature is enabled, the web application 502 may forward each URL request to a URL rewriter application 504. The rewriter application 504 may check the origin of the URL request. If the request does not originate from a “master” mode browser application instance 500 (e.g., from a predetermined, fixed IP address that is generally always assigned to a “master” mode browser application

12

instance) but rather comes from a “non-master” browser application instance 501, the rewriter application 504 may return a rewritten URL (e.g., the originally requested URL) to the web application 502, which may obtain the contents of the requested URL and forward the contents to the “non-master” browser application instance 501. It should be understood that in some embodiments, the web application 502 may also be configured to determine whether a URL request comes from a “private” mode browser application instance or a “secure-bookmark” mode browser application instance if these instances are configured to allow a secure bookmark to be selected or accessed.

When the URL request originates from a “master” mode browser application instance 500, the rewriter application 504 may determine if the requested URL corresponds to a “secure bookmark.” In particular, as described above, the rewriter 504 may determine if the requested URL corresponds with a URL stored in the shared preference directory 118 that is specified as a “secure bookmark.” If the requested URL doesn’t correspond with a previously-specified “secure bookmark,” the rewriter application 504 may return a rewritten URL (e.g., the originally requested URL) to the web application 502, which may obtain the contents of the requested URL and may forward the contents to the “master” mode browser application instance 500.

If, however, the URL request from the “master” mode browser application instance 500 corresponds to a previously-specified “secure bookmark,” the rewriter application 504 may return a rewritten URL to the web application 502. The rewritten URL may redirect the “master” mode browser application instance 500 making the request to a website or message indicating that a new “secure-bookmark” mode browser application instance has been launched for a requested “secure bookmark.” In some embodiments, the rewritten URL may be served by a local web computer or server (e.g., a tiny hypertext transfer protocol web server).

As shown in FIG. 5, if the URL request from the “master” mode browser application instance 500 corresponds to a previously-specified “secure bookmark,” the rewriter application 504 may also send the requested “secure bookmark” URL to a backend application or daemon 506. The daemon application 506 may be included in the VCCA 205. Upon receiving the secure bookmark URL, the daemon application 506 may invoke an application or script that creates a new VBE 208 within the virtual computer 202 and specifies the requested “secure bookmark” URL as the initial URL to access (e.g., as an input parameter). As described above, the browser application instance running with the new VBE 208 may be a “secure-bookmark” mode browser application instance, which may be assigned a different IP address than a “master” mode browser application instance.

To access the “secure bookmark,” the “secure-bookmark” mode browser application instance executed with the new VBE 208 may send the requested URL to the web application 502, which may forward the request to the rewriter application 504. However, because the requesting instance is a “secure-bookmark” mode browser application instance (i.e., a “non-master” browser application instance) rather than a “master” mode browser application instance, the rewriter application 504 may not determine whether the requested URL corresponds to a secure bookmark, but may simply return a rewritten URL (e.g., the originally requested URL) to the web application 502. The web application 502 may use the returned URL to obtain the contents of the requested URL and forward the contents to the “secure-bookmark” mode browser application instance executing within the new VBE 208.

US 8,839,422 B2

13

Returning to FIG. 4, after a browser application 304 executing within a VBE 208 accesses a website (e.g., the initial URL at 408, the desired non-secure-bookmark website at 414, or the desired secure bookmark website at 418), the VCMA 206 may monitor the behavior or operation of each VBE 208 and may provide information about the operation of each VBE 208 to the VCA 116 (at 420). The information about each VBE's operation may include the websites accessed by the browser application 304 and the browser application's interaction with the guest operating system 203. For example, the VCMA 206 may monitor and keep track of when the browser application 304 downloads one or more files, uploads one or more files, executes or attempts to execute another application, attempts to communicate with other applications within the VBE 208, accesses or attempts to access a particular application or particular data stored within the memory modules of the hardware 112, attempts to contact other computers connected to the computer 102 over at least one network, etc. As described above with respect to FIG. 3, the browser application 304 executed within each VBE 208 may include a browser helper application 306. The browser helper application 306 may collect all or a portion of the operational information provided to the VCMA 206, and ultimately provided to the VCA 116. For example, the browser helper application 306 may keep track of each URL accessed by the browser application 304. In some embodiments, the browser helper application 306 may store the URLs accessed by the browser application 304 to the shared preference directory 118 in addition to or in place of providing this information to the VCMA 206. The VCA 116 may then access the URL information from the shared preference directory 118 when the VCA 116 needs the information.

The VCA 116 may use the information about each VBE's operation to determine whether the operation of a particular VBE 206 indicates that potential malicious activity is occurring within the VBE 208 (at 422). Because in some embodiments the browser application 304 is the only application executed within a particular VBE 208, the VCA 116 may use the information about a VBE's operation to determine whether the operation is consistent or inconsistent with the normal operations of a browser application 304. For example, the VCA 116 may be configured with a set of "normal" interactions between a browser application and an operating system, set as caching data and creating and managing cookies. If the operation occurring with a particular VBE 208 is something other than these identified "normal" interactions, the VCA 116 may flag the operation or interaction as potential malicious activity.

Therefore, the isolation and specialized use of a VBE 208 may allow the VCA 116 to easily detect potential malicious activity. In particular, when a browser application 304 is executed directly within the computer 304 rather than within a virtual environment (e.g., a VBE 208), the "normal" operations requested of and performed by the computer's host operating system 114 may include many types of operations. For example, the host operating system 114 may execute multiple executable files, may store a file or data, may access one or more files or data, may modify a system file associated with the operating system, etc. This large range of "normal" operation occurs because many different applications may be simultaneously executed by the host operating system 114 within the computer 102. However, because the sole application executed with the VBE 208 may be the browser application 304, the types of "normal" or legitimate operations may be more limited, which may make it easier to detect potential malicious activity or operation.

14

In addition, if the VCA 116 detects potential malicious activity, the VCA 116 may terminate and automatically restore virtual computer 202, one or more VBEs 208, one or more instances of the browser application 304, or combinations thereof, (at 424) which kills the potential malicious activity before it may cause damage. This type of termination generally cannot be efficiently performed at the computer-level for each potential malicious activity because it would require termination and rebooting of the entire computer 102. Accordingly, using the VBEs 208 to execute the browser application 304 may allow the VCA 116 to better detect potential malicious activity and may allow the VCA 116 to react quickly and efficiently without requiring a reboot of the entire computer 102. Therefore, even if the potential malicious activity isn't truly malicious activity, the VCA 116 hasn't required a user to completely reboot the computer 102 but has only required the user to create a new VBE 208 and execute a new instance of the browser application 304 within the new VBE. In addition, as described above, in some embodiments, the VCA 116 may use a "snapshot" of the virtual computer 202 and/or a "snapshot" of a "pristine" VBE 208 to further increase the speed and efficiency of creation a new virtual computer 202 and/or a new VBE 208 quickly after the VCA 116 detected potential malicious activity and terminated these components.

As described below with respect to FIGS. 11 and 12, in some embodiments, the VCA 116 may only terminate and restore the virtual computer 202, one or more VBEs 208, one or more instances of the browser application 304, or combinations thereof if the user manually requests the termination. In other embodiments, the VCA 116 may automatically terminate one or more components of the computer 102 after it detects potential malicious activity either immediately or after a predetermined amount of time. In addition, the VCA 116 may be set to automatically terminate one or more components of the computer 102 after a predetermined time period regardless of whether potential malicious activity has been detected. For example, the VCA 116 may automatically terminate the virtual computer 202 and/or a VBE 208 if the component has been active for more than predetermined amount of time (e.g., 1 to 5 hours).

In some embodiments, after terminating one or more components of the computer 102 due to potential malicious activity, the VCA 116 may also collect information about the potential malicious activity and send the information to the collection computer 108 (at 424). The collected information may include one or more URLs where the potential malicious activity potentially originated from. The VCA 116 may obtain the one or more URLs associated with the detected potential malicious activity based on the information gathered by the browser helper application 306. If a browser application instance accesses one URL at a time, the VCA 116 may time-correlate the particular URL associated with the detected malicious activity. However, if multiple instances or windows of a browser application 304 are executing simultaneously, the VCA 116 may perform time-correlation heuristics to correlate the potential malicious activity to one or more potential URLs accessed approximately at the same time the potential malicious activity occurred. For example, assume a user accessed the following emails at the following time: www.goosite.com (11:29 a.m.); www.badsite.com (11:30 a.m.); and www.other.com (11:32 a.m.). If the VCA 116 determines that a potential malicious attack, such as a modification to a system file, occurred at 11:30 a.m., the VCA 116 may determine that the website www.badsite.com, accessed by the user at 11:30, is probably the source of the malicious attack. The time correlation heuristics may identify multiple

US 8,839,422 B2

15

URLs as potentially associated with the potential malicious activity, and, in some embodiments, the VCA 116 may allow a user to manually modify the one or more URLs identified as the source of potential malicious activity.

The collected information may also include forensic information about what the potential malicious activity did while running in the VBE 208 (e.g., all reads and writes performed on any files, all modifications or attempted modifications to registry entries, and all network communications). The collected information may also include configuration settings. For example, the version of browser application 340 executed within the VBE 208 and information about the host computer 102, such as its hardware configuration, may be included in the collected information. In general, any information that may help understand and identify malicious attempt may be included in the collected information. In some embodiments, private information may be stripped from the collected information before it is sent to the collection computer 108.

The collected information may also include information about the potential malicious activity, such as a signature of an executable downloaded or executed by the browser application 304. In some embodiments, the VCA 116 may only send the collected information about potential malicious activity to one or more collection computers 108 if the user provides permission. User permission may be provided on a case-by-case basis (e.g., by prompting the user to designate whether to send the collected information each time the VCA 116 detects potential malicious activity) or as a preconfigured preference for the VCA 116. The VCA 116 may also store the collected information and may use the collected information to automatically block a browser application from subsequently accessing a URL previously associated with malicious activity or to alert a user that a desired website was previously associated with malicious activity. In addition, the VCA 116 may be configured to display a list of URLs previously associated with malicious activity to a user.

The collection computer 108 may store the collected information about potential malicious activity to a database included in the collection computer 108 or to an external database. In order to mitigate the effects of a user who attempts to launch a denial of service (“DoS”) attack, the collection computer 108 may limit the amount of information or traffic received from a given user to a maximum amount (e.g., a maximum amount of information per day). The collection computer 108 may use the collected information about the potential malicious activity to identify new malicious activity present on the network 104. For example, the collection computer 108 may provide the collected malicious activity information to security organizations, such as the Anti-Phishing Group or OpenDNS to label certain URLs, files, or executables as being associated with malicious activity. This functionality may allow the collection computer 108 to provide zero-day malicious activity detection. This functionality may also be based on a human user’s real-world use of a browser application rather than on an automated application designed to crawl a network and detect malicious, which is what many current security organization use to identify malicious. In addition, if the collection computer 108 receives collected malicious activity information from multiple computers 102, the system 100 may provide a distributed continuous malicious activity detection system based on human, rather than automated behavior.

FIGS. 6-12 illustrate various user interfaces generated by the system 100. For example, FIG. 6 illustrates a user interface 600 that allows a user to select preferences for the VCA 116. As shown in FIG. 6, a user (e.g., an administrator) may use the interface 600 to specify how the VCA 116 should

16

create the virtual computer 202. In particular, a user may use a startup selection mechanism 602 (e.g., a check box) to specify whether the VCA 116 should create the virtual computer 202 in the background when the host operating system 114 is started or booted. A user or administrator may also use the interface 600 to set the browser application 304 that will be executed within a VBE 208 as the default browser application using a set-as-default selection mechanism 604 (e.g., a button). It should be understood that the user interface 600 may allow a user or an administrator to set other preferences for the VCA 116, such as a default browser mode (e.g., “master” mode or “private” mode), preferences setting how the VCA 116 should restore one or more VBEs 208 after they are terminated, how long VBEs 208 should be active before they are automatically terminated, what type of interaction or operation within a VBE 208 is associated with potential malicious activity, what actions to take upon detecting potential malicious activity, etc.

FIG. 7 illustrates a user interface 700 that allows a user to select a secure bookmark within a browser application according to one embodiment of the invention. As shown in FIG. 7, the interface 700 may include a bookmark drop-down menu 702. The bookmark drop-down menu 702 may include a secure bookmarks folder 704 that lists one or more websites, such as 706, previously designated as a “secure bookmark.” As described above with respect to FIGS. 4 and 5, if a user selects a website specified as “secure bookmark” from the bookmark drop-down menu 702, the VCCA 205 may create a new VBE 208 and may execute the browser application 304 within the new VBE 208 in a “secure-bookmark” mode.

FIG. 8 illustrates a user interface 800 that displays a “secure bookmark” within a “secure-bookmark” mode browser application 304 according to one embodiment of the invention. As shown in FIG. 8, the navigation tools of the browser application 304, such as an address line 802, may be disabled in order to prevent the browser application 304 from being redirected to another, potentially unsecure website. For example, as described above, the address line 802 may be set to be read-only, which prevents a user from typing in a URL for the browser application to access. As also shown in FIG. 8, the interface 800 may not include a bookmark drop-down menu, a history drop-down menu, a home selection mechanism, etc. Again, as described above, these features may be disabled (i.e., removed from the interface 800) in order to prevent a user from navigating the browser application to another, potentially unsecure, website.

FIG. 9 illustrates a user interface 900 that displays a website 902 within a browser application 304 and displays a health monitor 904 according to one embodiment of the invention. As shown in FIG. 9, the health monitor 904 may display information to a user about the status of the browser application 304 and/or the VBE 208 executing the browser application 304. The displayed information may include a visual depiction of a health status 905 (e.g., a green light for “healthy,” a yellow light for “caution,” and a red light for “warning” or “unhealthy”). The displayed information may also include an amount of time that the VBE 208 and/or the browser application 304 has been active or running. In addition, the health monitor 904 may include a restore selection mechanism 906 (e.g., a button) and a terminate selection mechanism 908 (e.g., a button). A user may select the restore selection mechanism 906 to terminate the browser application 304 and/or the VBE 208 executing the browser application 304 and automatically create a new instance of the browser application 304 and/or a new VBE to execute the new browser application instance. Similarly, a user may select the terminate selection mechanism 908 to terminate the browser

US 8,839,422 B2

17

application **304** and/or the VBE **208** executing the browser application **304** without automatically creating a new instance of the browser application **304** and/or a new VBE **208** for executing the new browser application instance.

FIG. 10 illustrates another health monitor **1000** according to one embodiment of the invention. As shown in FIG. 10, the health monitor **1000** may include a visual depiction **1002** of the health of the browser application **304** and/or the VBE **208** executing the browser application **304**, such as a green light, a yellow light, or a red light. The health monitor **1000** may also include a textual depiction of the health of the browser application **304** (e.g., “Good,” “Infection Detected,” etc.). As shown in FIG. 10, the health monitor **1000** may also include a restore selection mechanism **1004** (e.g., a button) and an open-browser selection mechanism **1006** (e.g., a button). A user may select the restore selection mechanism **1004** to terminate the browser application **304** and/or the VBE **208** executing the browser application **304** and automatically create a new instance of the browser application **304** and/or a new VBE **208** for executing the new browser application instance. Similarly, a user may select the open-browser selection mechanism **1006** to create a new instance of the browser application **304** within a new VBE **208** if one is not already running within the VBE **208**. For example, a user may use the open-browser selection mechanism to open a “master” mode browser instance if one is not already running. It should be understood that the health monitors **904** and **1000** may be positioned in the same interface or window as a website displayed by the browser application **304** or may be part of a separate interface or window.

FIGS. 11 and 12 illustrate user interfaces that display alerts to a user regarding a browser application and/or the VBE **208** executing the browser application **304** according to some embodiments of the invention. For example, FIG. 11 illustrates a user interface **1100** that may alert a user that potential malicious activity (i.e., a potential “infection”) has been detected by the VCMA **206**. The user interface **1100** may also include a restore selection mechanism **1102** (e.g., a button). As instructed in the message within the interface **1100**, a user may select the restore selection mechanism **1102** to terminate the browser application **304** and/or the VBE **208** executing the browser application **304** and automatically create a new instance of the browser application **304** and/or a new VBE **208** to execute the new browser application instance. FIG. 12 illustrates another user interface **3040** that may alert a user that potential malicious activity has occurred in the form of the downloading of an executable file. The user interface **3040** may also instruct a user to restore (i.e., terminate and restart) the browser application **304** and/or the VBE **208** where the download occurred if the user did not intend to download the executable file.

It should be understood that the user interfaces **1100** and **3040** may be positioned in the same interface or window as a website displayed by the browser application **304** or may be part of a separate interface or window. Additionally, in some embodiments, the user interface **1100** and **3040** may inform a user that the browser application **304** and/or the VBE **208** executing the browser application **304** will be automatically restored rather than instructing a user to perform the restoration manually. For example, the user interfaces **1100** and **3040** may include a message that the browser application **304** and/or the VBE **208** executing the browser application **304** will automatically be restored after a predetermined period of time. The user interfaces **1100** and **3040** may also include a timer showing the time remaining before an automatic restoration is performed.

18

It should be understood that although embodiments of the invention have been described with respect to a browser application **304**, the embodiments may be used with other types of applications. In particular, the VBEs **208** may be used to isolate the execution of any type of application. For example, a separate VBE **208** may be used to execute any application downloaded from another computer (e.g., over the Internet), any application that includes an invalid or unverifiable certificate, any application executed on a public computer, any user-initiated application, or combinations thereof.

In this specification, “a” and “an” and similar phrases are to be interpreted as “at least one” and “one or more.”

The disclosure of this patent document incorporates material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, for the limited purposes required by law, but otherwise reserves all copyright rights whatsoever.

Before embodiments of the invention are described in detail, it should be understood that the terms “computer,” “database,” “application,” and “module” can represent hardware, or software in combination with hardware. In addition, the computers, databases, applications, and modules described herein can be implemented on standard, general-purpose computers or as specialized devices.

While various embodiments have been described above, it should be understood that they have been presented by way of example, and not limitation. It will be apparent to persons skilled in the relevant art(s) that various changes in form and detail may be made therein without departing from the spirit and scope. In fact, after reading the above description, it will be apparent to one skilled in the relevant art(s) how to implement alternative embodiments. Thus, the present embodiments should not be limited by any of the above described example embodiments.

In addition, it should be understood that any figures which highlight the functionality and advantages, are presented for example purposes only. The disclosed architecture is sufficiently flexible and configurable, such that it may be utilized in ways other than that shown. For example, the steps listed in any flowchart may be re-ordered or only optionally used in some embodiments.

Further, the purpose of the Abstract of the Disclosure is to enable the U.S. Patent and Trademark Office and the public generally, and especially the scientists, engineers and practitioners in the art who are not familiar with patent or legal terms or phraseology, to determine quickly from a cursory inspection the nature and essence of the technical disclosure of the application. The Abstract of the Disclosure is not intended to be limiting as to the scope in any way.

Finally, it is the applicant’s intent that only claims that include the express language “means for” or “step for” be interpreted under 35 U.S.C. 112, paragraph 6. Claims that do not expressly include the phrase “means for” or “step for” are not to be interpreted under 35 U.S.C. 112, paragraph 6.

What is claimed is:

1. A tangible non-transitory processor-readable medium containing instructions that when executed by one or more processors, performs a method comprising:
upon initiation of at least one browser application, creating at least one virtual browsing environment with at least one operating system and executing the at least one browser application within the at least one virtual browsing environment;

US 8,839,422 B2

19

monitoring operation of the at least one operating system within the at least one virtual browsing environment; determining when an operation of the at least one operating system within the at least one virtual browsing environment includes potential malicious activity; terminating the at least one virtual browsing environment when the operation includes potential malicious activity; and transmitting information to at least one collection computer about potential malicious activity when the operation of the at least one operating system of the at least one virtual browsing environment includes potential malicious activity, the information including at least one website address and an indication of an operation of the at least one operating system when the at least one browser application executed within the at least one virtual browsing environment accessed at least one website at the at least one website address.

2. The tangible non-transitory processor-readable medium of claim 1, wherein the method further comprises displaying information about potential malicious activity to at least one user when the operation of the at least one operating system of the at least one virtual browsing environment includes potential malicious activity.

3. The tangible non-transitory processor-readable medium of claim 1, wherein the method further comprises creating at least one second virtual browsing environment after terminating the at least one virtual browsing environment.

4. The tangible non-transitory processor-readable medium of claim 3, wherein the method further comprises taking at least one snapshot of the at least one virtual browsing environment upon creation.

5. The tangible non-transitory processor-readable medium of claim 4, wherein the creating the at least one second virtual browsing environment after terminating the at least one virtual browsing environment includes restoring the at least one virtual browsing environment using the at least one snapshot.

6. The tangible non-transitory processor-readable medium of claim 1, wherein the method further comprises terminating the at least one virtual browsing environment after at least one predetermined period of time.

7. The tangible non-transitory processor-readable medium of claim 1, wherein the method further comprises receiving a website selection within the at least one browser application and determining if the website selection corresponds to a website specified as a secure bookmark.

8. The tangible non-transitory processor-readable medium of claim 7, wherein the method further comprises:

when the website selection corresponds to a website specified as a secure bookmark, creating at least one second virtual browsing environment with at least one operating system, executing at least one browser application within the at least one second virtual browsing environment, and accessing the website selection within the at least one browser application executed within the at least one second virtual browsing environment.

9. The tangible non-transitory processor-readable medium of claim 1, wherein the at least one operating system of the at least one virtual browsing environment includes at least one virtualized operating system sharing at least one kernel of at least one supporting operating system.

10. The tangible non-transitory processor-readable medium of claim 9, wherein the method further comprises creating at least one virtual computer including the at least one supporting operating system with the at least one kernel and creating the at least one virtual browsing environment within the at least one virtual computer.

20

11. A tangible non-transitory processor-readable medium containing instructions that when executed by one or more processors perform a method comprising:

upon initiation of at least one browser application, creating at least one first virtual browsing environment with at least one operating system and executing the at least one browser application within the at least one first virtual browsing environment;

receiving a website selection within the at least one browser application; determining if the website selection corresponds to a website specified as a secure bookmark;

when the website selection corresponds to a website specified as a secure bookmark, creating at least one second virtual browsing environment with at least one operating system, executing at least one browser application within the at least one second virtual browsing environment, and accessing the website selection within the at least one browser application executed within the at least one second virtual browsing environment; and when the website selection does not correspond to a website specified as a secure bookmark, accessing the website selection with the at least one browser application executed within the at least first virtual browsing environment.

12. The tangible non-transitory processor-readable medium of claim 11, wherein the method further comprises modifying the at least one browser application executed within the at least one second virtual browsing environment to prevent the at least one browser application executed within the at least one second virtual browsing environment from being directed to a website different from the website selection.

13. The tangible non-transitory processor-readable medium of claim 12, wherein the modifying the at least one browser application includes setting an address line of the at least one browser application executed within the at least one second virtual browsing environment to be read-only.

14. The tangible non-transitory processor-readable medium of claim 12, wherein the modifying the at least one browser application includes disabling toolbar options within the at least one browser application executed within the at least one second virtual browsing environment that allow a user to select a website to access.

15. The tangible non-transitory processor-readable medium of claim 11, wherein the determining if the website selection corresponds to a website specified as a secure bookmark includes comparing the website selection to at least one file of secure bookmarks.

16. The tangible non-transitory processor-readable medium of claim 15, wherein the method further comprises receiving at least one indication to set the website as a secure bookmark and updating the at least one file of secure bookmarks based on the at least one indication.

17. The tangible non-transitory processor-readable medium of claim 11, wherein the at least one operating system of the at least one first virtual browsing environment and the at least one operating system of the at least one second virtual browsing environment include at least one virtualized operating system sharing at least one kernel of at least one supporting operating system.

18. The tangible non-transitory processor-readable medium of claim 17, wherein the method further comprises creating at least one virtual computer including the at least one supporting operating system with the at least one kernel and creating the at least one first virtual browsing environ-

US 8,839,422 B2

21

ment and the at least one second virtual browsing environment within the at least one virtual computer.

19. The tangible non-transitory processor-readable medium of claim **11**, wherein the method further comprises monitoring operation of the at least one operating system within the at least one second virtual browsing environment, determining if the operation of the at least one operating system within the at least one second virtual browsing environment includes potential malicious activity, and terminating the at least one second virtual browsing environment ⁵ when the operation includes potential malicious activity. ¹⁰

20. A tangible non-transitory processor-readable medium containing instructions that when executed by one or more processors, performs a method comprising:

upon initiation of at least one browser application, creating ¹⁵ at least one virtual browsing environment with at least one operating system and executing the at least one browser application within the at least one virtual browsing environment;

taking at least one snapshot of the at least one virtual ²⁰ browsing environment upon creation;

monitoring operation of the at least one operating system within the at least one virtual browsing environment;

22

determining when the operation of the at least one operating system within the at least one virtual browsing environment includes potential malicious activity; terminating the at least one virtual browsing environment when the operation includes potential malicious activity; transmitting information to at least one collection computer about potential malicious activity when the operation of the at least one operating system within the at least one virtual browsing environment includes potential malicious activity, the information including at least one website address and an indication of an operation of the at least one operating system when the at least one browser application executed within the at least one virtual browsing environment accessed at least one website at the at least one website address; creating at least one second virtual browsing environment after terminating the at least one virtual browsing environment; and restoring the at least one virtual browsing environment using the at least one snapshot.

* * * * *